(12)特許協力条約に基づいて公開された国際

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年2 月3 日 (03.02.2005)

PCT

(10) 国際公開番号
WO 2005/010770 A1

(51) 国際特許分類[7]: G06F 15/00, H04L 9/32

(21) 国際出願番号: PCT/JP2004/009256

(22) 国際出願日: 2004 年6 月24 日 (24.06.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-281348 2003 年7 月28 日 (28.07.2003) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 中野 雄彦 (NAKANO, Takehiko) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP). 嶋 久登 (SHIMA, Hisato) [JP/JP]; 〒1410001 東京都品川区北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

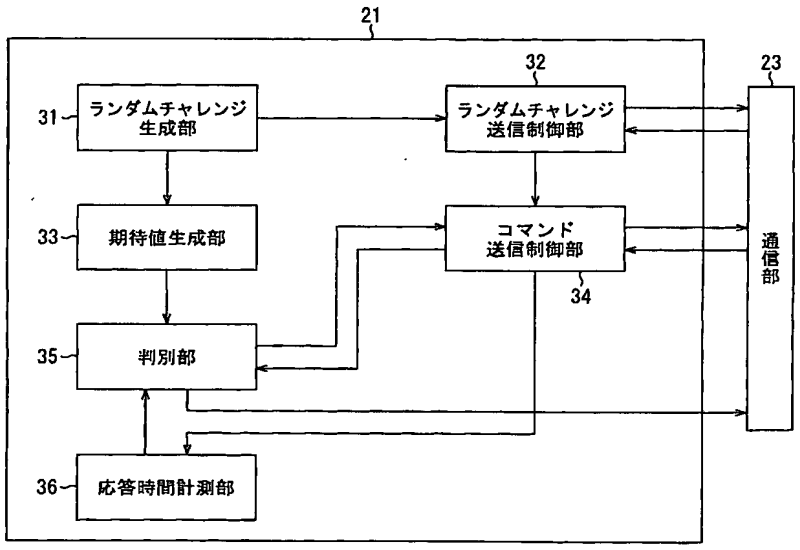
(74) 代理人: 稲本 義雄 (INAMOTO, Yoshio); 〒1600023 東京都新宿区 西新宿７丁目１１番１８号 ７１１ビルディング４階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE AND METHOD, RECORDING MEDIUM, AND PROGRAM

(54) 発明の名称: 情報処理装置および方法、記録媒体、並びにプログラム



31...RANDOM CHALLENGE GENERATION SECTION
32...RANDOM CHALLENGE TRANSMISSION CONTROL SECTION
33...EXPECTATION VALUE GENERATION SECTION
34...COMMAND TRANSMISSION CONTROL SECTION
35...JUDGMENT SECTION
36...RESPONSE TIME MEASUREMENT SECTION
23...COMMUNICATION SECTION

(57) Abstract: There is provided an information processing device capable of appropriately communicating with a communication partner according to a communication time with the partner. A reception control section (41) receives a random challenge (RC) from a terminal (11) of a transmission side and supplies it to a generation section (42). The reception control section (41) transmits an RC reception message indicating that an RC has been received, to the transmission side. The generation section (42) subjects the RC to hash processing and supplies the authentication data obtained as a result to a generation section (43). At a timing before receiving a response request command from the transmission side, a transmission control section (44) controls the generation section (43) so as to generate a response message containing authentication data corresponding to the response request command and, upon reception of the response request command, transmits the response message to the terminal of the transmission destination. The present invention can be applied to a content providing system.

(57) 要約: 本発明は、相手との通信時間に基づいて、通信相手と適切に通信することができるようにした情報処理装置に関する。受信制御部４１は、送信側の端末１１からのランダムチャレンジ（ＲＣ）を受信し、生成部４２に供給する。受信制御部４１はＲＣを受信した旨を表すＲＣ受信メッセージを送信側に送信する。生成部４２は、ＲＣに対してハッシュ処理を施し、その結果得られた認証データを生成部４３に供給する。送信制御部４４は、送信側からの応答要求コマンドを受信する前のタイミングで、生成部４３を制御して、応答要求コマンドに

[続葉有]

WO 2005/010770 A1

BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

対応した認証データを含む応答メッセージを生成させるとともに、応答要求コマンドを受信したとき、その応答メッセージを送信先の端末に送信する。本発明は、コンテンツ提供システムに適用することができる。

明細書

情報処理装置および方法、記録媒体、並びにプログラム

技術分野

本発明は、情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、通信相手との通信時間を適切に計測することができるようにした情報処理装置および方法、記録媒体、並びにプログラムに関する。

背景技術

近年、インターネットに代表される公共性のある広域に亘るネットワーク（以下、WAN(Wide Area Network)と称する）や一般家屋等に設けられる局所的なネットワーク（以下、LAN(Local Area Network)と称する）の普及に伴い、それらのネットワークを介した各種データ通信が盛んに行われている。

映像や音楽コンテンツなどを、ネットワークを通して伝送する場合は、著作権保護のために、通信相手の機器との間で、認証および鍵交換を行い、コンテンツを暗号化して伝送することが行われている（下記の文献参照）。

DTCP Specification Volume 1 Version 1.3 (Information Version)
http://www.dtcp.com/daTa/info_20040107_dtcp_Vol_1_1p3.pdf

ここにおいて、著作権の観点からは、家庭内でのコピーや伝送は許可するが、WAN で接続された他の家庭との間でのコンテンツの伝送を制限したい場合がある。例えば、テレビジョン放送を録画したコンテンツは、私的利用の範囲（家庭内）で利用できるが、インターネットを通して、他人に伝送するのは著作権を侵害すると考えられるので、このような制限が必要となる。

この制限の下では、著作権保護されたコンテンツを送信する機器(送信機器)は、そのコンテンツを受信する通信相手の機器(受信機器)が同一 LAN 内にあるか、WAN(インターネット)を通して接続されているかを判断する必要がある。

例えば、IP アドレスから通信相手が同一サブネット内にあるかどうかを調べる

ことや、IP通信パケットが通過したIPルータの数(Hop Count)を使うことで通信相手がWAN(インターネット)を通して接続されているかを知ることができる。しかしながら、WAN(インターネット)を経由した通信であってもVPN(Virtual Private Network)などの技術を使えば、IPルータを経由せずに接続されている同一サブネットであるかように接続することが可能である。すなわち不正にコンテンツを入手することが可能である。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、所定のコマンドに対する受信機器の応答時間に基づいて通信距離を判別し、例えば送信機器と同一LANに接続されているか否かを判定することを目的とする。

本発明の第1の情報処理装置は、受信装置との間で共有する共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信手段と、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証手段と、受信装置からの、コマンドに対する応答時間を計測する計測手段と、認証手段による認証結果、および計測手段により計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定手段とを備えることを特徴とする。

コマンド送信手段は、データの送信可否を判定するのに、コマンドを最大N回送信し、認証手段は、コマンドの送信の順番に応じた認証データとその期待値とに基づいて、受信装置を認証することができる。

本発明の第1の情報処理方法は、受信装置との間で共有する共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、認証ステップでの認証結果、および計測ステップの処理で計測された応答時間に基づい

て、受信装置に対するデータの送信可否を判定する判定ステップとを含むことを特徴とする。

本発明の第１の記録媒体のプログラムは、受信装置との間で共有する共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置に対する送信を制御するコマンド送信制御ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づく受信装置の認証を制御する認証制御ステップと、受信装置からの、コマンドに対する応答時間の計測を制御する計測制御ステップと、認証制御ステップでの認証結果、および計測制御ステップの処理で計測された応答時間に基づく、受信装置に対するデータの送信可否の判定を制御する判定制御ステップとを含むことを特徴とする。

本発明の第１のプログラムは、受信装置との間で共有する共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置に対する送信を制御するコマンド送信制御ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づく受信装置の認証を制御する認証制御ステップと、受信装置からの、コマンドに対する応答時間の計測を制御する計測制御ステップと、認証制御ステップでの認証結果、および計測制御ステップの処理で計測された応答時間に基づく、受信装置に対するデータの送信可否の判定を制御する判定制御ステップとを含む処理をコンピュータに実行させることを特徴とする。

本発明の第１の情報処理装置および方法、並びにプログラムにおいては、受信装置との間で共有する共有データに基づいて認証データが生成された後、応答を要求するコマンドが受信装置に送信され、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置が認証され、受信装置からの、コマンドに対する応答時間が計測され、認証結果、および応答時間に基づいて、受信装置に対するデータの送信可否が判定される。

本発明の第２の情報処理装置は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成

手段と、認証データ生成手段により生成された認証データを含む、コマンドに対する応答メッセージを、送信装置からコマンドが送信されてくる前に生成する応答メッセージ生成手段と、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信手段とを備えることを特徴とする。

共有データは、疑似乱数であるようにし、疑似乱数は、コマンドの前に送信装置から送信されるようにし、認証データ生成手段は、疑似乱数に対して鍵付きハッシュ処理を施し、その結果得られたハッシュ値を認証データとすることができる。

認証データ生成手段は、疑似乱数と情報処理装置固有の情報に対して、鍵付きハッシュ処理を施し、その結果得られたハッシュ値を認証データとすることができる。

データの送信可否を判定するのに、送信装置から、コマンドが最大N回送信されてくる場合において、認証データ生成手段は、送信装置から最初のコマンドが送信されてくる前に、共有データに対して処理を施して、送信されてくるN個のコマンドのそれぞれに対応するN個の認証データを生成し、送信手段は、N個の認証データが、送信装置と予め合意した順番で送信装置に提供されるように、応答メッセージ生成手段により生成された応答メッセージを送信装置に送信することができる。

認証データ生成手段は、共有データに対して処理を施して得られたデータを複数個に分割し、分割されたデータからN個の認証データを生成することができる。

認証データ生成手段は、共有データに対して処理を繰り返し施し、その処理毎に得られたデータから、N個の認証データを生成することができる。

送信手段は、送信装置からのコマンドが受信されたとき、認証データとコマンドに含まれる情報から生成された新たな認証データを含む応答メッセージを、送信装置に送信することができる。

本発明の第２の情報処理方法は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成

ステップと、認証データ生成ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージを、送信装置からコマンドが送信されてくる前に、生成する応答メッセージ生成ステップと、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信ステップとを含むことを特徴とする。

本発明の第２の記録媒体のプログラムは、送信装置からコマンドが送信されてくる前の、共有データに対して所定の処理を施しての認証データの生成を制御する認証データ生成制御ステップと、送信装置からコマンドが送信されてくる前の、認証データ生成制御ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、送信装置から送信されてきたコマンドが受信されたときの、応答メッセージの送信装置に対する送信を制御する送信制御ステップとを含むことを特徴とする。

本発明の第２のプログラムは、送信装置からコマンドが送信されてくる前の、共有データに対して所定の処理を施しての認証データの生成を制御する認証データ生成制御ステップと、送信装置からコマンドが送信されてくる前の、認証データ生成制御ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、送信装置から送信されてきたコマンドが受信されたときの、応答メッセージの送信装置に対する送信を制御する送信制御ステップとを含むことを特徴とする。

本発明の第２の情報処理装置および方法、並びにプログラムにおいては、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データが生成され、送信装置からコマンドが送信されてくる前に、生成された認証データを含む、コマンドに対する応答メッセージが生成され、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージが送信装置に送信される。

本発明の第３の情報処理装置は、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成手段と、コ

マンド認証データを含み、応答を要求するコマンドを受信装置に送信するコマンド送信手段と、コマンドに対する受信装置からの応答を受信する応答受信手段と応答期待値と、受信装置から受信した応答に含まれる応答認証データに基づいて受信装置を認証する認証手段と、受信装置からの、コマンドに対する応答時間を計測する計測手段と、認証手段による認証結果、および計測手段により計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定手段とを備えることを特徴とする。

コマンド送信手段は、データの送信可否を判定するのに、コマンドを最大k回送信し、認証手段は、コマンドの送信の順番に応じた認証データとその期待値とに基づいて、受信装置を認証することができる。

本発明の第3の情報処理方法は、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、コマンド認証データを含み、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、コマンドに対する受信装置からの応答を受信する応答受信ステップと、応答期待値と、受信装置から受信した応答に含まれる応答認証データに基づいて受信装置を認証する認証ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、認証ステップの処理での認証結果、および計測ステップにより計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定ステップとを含むことを特徴とする。

本発明の第3の記録媒体のプログラムは、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、コマンド認証データを含み、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、コマンドに対する受信装置からの応答を受信する応答受信ステップと、応答期待値と、受信装置から受信した応答に含まれる応答認証データに基づいて受信装置を認証する認証ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、認証ステップの処理での

認証結果、および計測ステップにより計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定ステップとを含むことを特徴とする。

本発明の第３のプログラムは、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、コマンド認証データを含み、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、コマンドに対する受信装置からの応答を受信する応答受信ステップと、応答期待値と、受信装置から受信した応答に含まれる応答認証データに基づいて受信装置を認証する認証ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、認証ステップの処理での認証結果、および計測ステップにより計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定ステップとを含む処理をコンピュータに実行させることを特徴とする。

本発明の第３の情報処理装置および方法、並びにプログラムにおいては、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データが生成され、コマンド認証データを含み、応答を要求するコマンドが受信装置に送信され、コマンドに対する受信装置からの応答が受信され、応答期待値と、受信装置から受信した応答に含まれる応答認証データに基づいて受信装置が認証され、受信装置からの、コマンドに対する応答時間が計測され、認証結果、および応答時間に基づいて、受信装置に対するデータの送信可否が判定される。

本発明の第４の情報処理装置は、送信装置との間で共有する共有データから、送信装置において共有データから生成されたコマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成手段と、送信装置から送信されてきたコマンドが受信されたとき、コマンドに含まれるコマンドの認証データと、生成手段により生成されたコマンド期待値データに基づいて送信装置を認証する認証手段と、認証手段による認証結果に基づいて、応答認証データを含む応答を送信装置に送信する送信手段とを備えることを特徴とする。

本発明の第４の情報処理方法は、送信装置との間で共有する共有データから、送信装置において共有データから生成されたコマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、送信装置から送信されてきたコマンドが受信されたとき、コマンドに含まれるコマンドの認証データと、生成ステップの処理で生成されたコマンド期待値データに基づいて送信装置を認証する認証ステップと、認証ステップの処理での認証結果に基づいて、応答認証データを含む応答を送信装置に送信する送信ステップとを備えることを特徴とする。

本発明の第４の記録媒体のプログラムは、送信装置との間で共有する共有データから、送信装置において共有データから生成されたコマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、送信装置から送信されてきたコマンドが受信されたとき、コマンドに含まれるコマンドの認証データと、生成ステップの処理で生成されたコマンド期待値データに基づいて送信装置を認証する認証ステップと、認証ステップの処理での認証結果に基づいて、応答認証データを含む応答を送信装置に送信する送信ステップとを含むことを特徴とする。

本発明の第４のプログラムは、送信装置との間で共有する共有データから、送信装置において共有データから生成されたコマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、送信装置から送信されてきたコマンドが受信されたとき、コマンドに含まれるコマンドの認証データと、生成ステップの処理で生成されたコマンド期待値データに基づいて送信装置を認証する認証ステップと、認証ステップの処理での認証結果に基づいて、応答認証データを含む応答を送信装置に送信する送信ステップとを含む処理をコンピュータに実行させることを特徴とする。

本発明の第４の情報処理装置および方法、並びにプログラムにおいては、送信装置との間で共有する共有データから、送信装置において共有データから生成されたコマンドの認証データに対応するコマンド期待値データおよび応答認証デー

タが生成され、送信装置から送信されてきたコマンドが受信されたとき、コマンドに含まれるコマンドの認証データと、生成されたコマンド期待値データに基づいて送信装置が認証され、その認証結果に基づいて、応答認証データを含む応答が送信装置に送信される。

図面の簡単な説明

図１は、本発明を適用した情報通信システムの利用例を示す図である。

図２は、図１の端末の構成例を示すブロック図である。

図３は、図２の送信可否判定部の構成例を示すブロック図である。

図４は、図２の応答制御部の構成例を示すブロック図である。

図５は、送信可否判定処理および応答処理を説明するフローチャートである。

図６は、期待値および認証データの生成方法を説明する図である。

図７は、期待値および認証データの他の生成方法を説明する図である。

図８は、図１の端末の動作を説明する図である。

図９は、図２の送信可否判定部の他の構成例を示すブロック図である。

図１０は、図２の応答制御部の他の構成例を示すブロック図である。

図１１は、他の送信可否判定処理を説明するフローチャートである。

図１２は、他の応答処理を説明するフローチャートである。

図１３は、図１の端末の動作を説明する他の図である。

図１４は、図１の端末の動作を説明する他の図である。

図１５は、図１の端末の動作を説明する他の図である。

図１６は、パーソナルコンピュータの構成例を示すブロック図である。

発明を実施するための最良の形態

図１は、本発明を適用した端末１１からなる情報通信システムの構成例を示している。

LAN１－１，１－２（以下、個々に区別する必要がない場合、単位、LAN１と称

する。他の場合についても同様である）がインターネットに代表される WAN２を介して相互に接続されている。

LAN１－１は、例えば、家屋内に設けられ、特定の個人（あるいは、家族）が使用する程度の規模のものであり、それには、スイッチングハブ（図示せず）を介して、パーソナルコンピュータやＡＶ機器等の端末１１－１および端末１１－２が接続されている。LAN１－１と端末１１－１および１１－２との接続は、例えば、Ethernet(登録商標)（100BASE-TX）等の高速インタフェースによる。端末１１－１および１１－２は、LAN１－１および WAN２を介して、LAN１－２に接続することができる。

LAN１－２は、LAN１－１と同様に構成されており、それには、端末１１－３が接続されている。

各端末１１は、本情報通信システムに登録された正規の機器であり、図２に示すように、送信可否判定部２１、応答制御部２２、通信部２３、および送信データ格納部２４を含んで構成されている。

送信可否判定部２１は、他の端末１１（受信側の端末１１）に所定のデータを送信する際に、通信部２３を介して、受信側の端末１１（正確には、その応答制御部２２）と後述するように通信することで、受信側の端末１１が本情報通信システムにおける正規の機器であるか否かを認証するとともに、所定の要求に対する受信側の端末１１の応答時間を、受信側の端末１１との通信時間として計測する。

送信可否判定部２１は、受信側の端末１１の認証結果および応答時間に基づく通信距離の判別結果に基づいて、受信側の端末１１に対するデータの送信可否を判定する。

例えば、受信側の端末１１が、送信側の端末１１と異なる LAN１に接続されている場合（WAN２を介して接続され、いわゆる通信距離が長い場合）、応答時間は、同じ LAN１に接続されている場合（通信距離が短い場合）に比べて長くなるので、例えば、通信が同一 LAN１内に制限されているとき、送信可否判定部２１は、計

測した応答時間から受信側の端末１１が送信側の端末１１と同じ LAN１に接続されているか否かを判定し、その判定結果と受信側の端末１１の認証結果に基づいて、データ送信の可否を判定する。

すなわち図１の例では、端末１１－１（送信側）が端末１１－２（受信側）にデータを送信する場合、端末１１－１の送信可否判定部２１は、計測した端末１１－２の応答時間から、端末１１－２が LAN１－１に接続されていることを判定し、データ送信を行う。一方、端末１１－１が端末１１－３にデータを送信する場合、端末１１－１の送信可否判定部２１は、計測した端末１１－３の応答時間から、端末１１－３は LAN１－１と異なる LAN（LAN１－２）に接続されていることを判定し、データ送信を行わない。

なおこのような通信距離による通信制御は、映画などのコンテンツを一定の地域に対して先行配給し、他の地域には後日配給するなどのコンテンツ配給ビジネスに適用することができる。

図２に戻り、応答制御部２２は、送信側の端末１１から所定のデータの送信を受ける際、通信部２３を介して、送信側の端末１１（正確には、その送信可否判定部２１）と後述するように通信することで、送信側の端末１１における認証および応答時間の適切な計測に必要な情報を送信側の端末１１に送信する。

通信部２３は、LAN１に接続されており、同一の LAN１内の端末１１、または WAN２を介して異なる LAN１に接続されている端末１１との通信を行う。

送信データ格納部２４は、受信側の端末１１に送信される、所定のデータが格納されている。

図３は、端末１１の送信可否判定部２１の構成例を示している。

ランダムチャレンジ生成部３１は、所定ビット数の疑似乱数（以下、ランダムチャレンジと称する）を生成し、ランダムチャレンジ送信制御部３２および期待値生成部３３に供給する。

ランダムチャレンジ送信制御部３２は、ランダムチャレンジ生成部３１から供給されたランダムチャレンジを、通信部２３を介して、受信側の端末１１に送信

する。ランダムチャレンジ送信制御部３２はまた、通信部２３を介して、受信側の端末１１から送信されてきた、ランダムチャレンジを受信した旨のメッセージ（以下、ＲＣ受信メッセージと称する）を受信し、そのときＲＣ受信メッセージを受信した旨をコマンド送信制御部３４に通知する。

期待値生成部３３は、ランダムチャレンジ生成部３１から供給されたランダムチャレンジに対して、例えば、受信側の端末１１と共有する秘密鍵を利用したHMAC（Keyed-Hashing for Message Authentication, IETF RFC 2104）アルゴリズムによるハッシュ処理（いわゆる鍵付きハッシュ処理）を施して、受信側の端末１１でランダムチャレンジから生成される認証データの期待値を生成し、判定部３５に供給する。期待値生成部３３はまた、端末１１に予め設定された端末１１固有の情報（例えば、機器ID）とランダムチャレンジを連結したものに鍵付きハッシュ処理を施して期待値を生成することもできる。

なお、ハッシュ処理で利用される秘密鍵は、本情報通信システムの正規の機器に所定のタイミングで安全に配信される。

コマンド送信制御部３４は、ランダム送信制御部３２から、ＲＣ受信メッセージを受信した旨が通知されたとき、または判定部３５からの指示に従って、応答を要求するコマンド（以下、応答要求コマンドと称する）を、通信部２３を介して、受信側の端末１１に送信する。

コマンド送信制御部３４または、通信部２３を介して、送信した応答要求コマンドに対する応答として、受信側の端末１１から送信されてきたメッセージ（以下、応答メッセージと称する）を受信し、それを判定部３５に供給する。応答メッセージには、ランダムチャレンジ送信制御部３２により送信されたランダムチャレンジから生成された認証データが組み込まれている。

コマンド送信制御部３４または、応答要求コマンドを送信した後、応答時間計測部３６を制御して、応答時間の計測を開始させるとともに、その応答要求コマンドに対する応答としての応答メッセージを受信したとき、応答時間の計測を終了させる。

判定部３５は、コマンド送信制御部３４からの応答メッセージに組み込まれている認証データと、期待値生成部３３で生成されたその認証データの期待値に基づいて、受信側の端末１１が、本情報通信システムにおける正規の機器であるかの認証を行う。判定部３５はまた、応答時間計測部３６で計測された応答時間が所定の時間 TL を越えているか否かを判定して、通信距離の判別（送信側の端末１１と同一の LAN1 に接続されているかの判定）を行う。

判定部３５は、受信側の端末１１の認証結果および通信距離の判別結果に基づいて、データの送信可否の判定を行う。判定部３５は、その判定結果に基づいて、通信部２３を制御し、送信データ格納部２４に格納されているデータを、受信側の端末１１に送信させる。

応答時間計測部３６は、コマンド送信制御部３４からの指示に従って、内蔵するタイマを動作させ、受信側の端末１１の応答時間を計測する。

図４は、端末１１の応答制御部２２の構成例を示している。

ランダムチャレンジ受信制御部４１は、通信部２３を介して、送信側の端末１１（正確には、その送信可否判定部２１）から送信されてきたランダムチャレンジを受信し、それを認証データ生成部４２に供給する。ランダムチャレンジ受信制御部４１はまた、通信部２３を介して、ＲＣ受信メッセージ（ランダムチャレンジを受信した旨を表すメッセージ）を、送信側の端末１１に送信し、そのときＲＣ受信メッセージを送信した旨を応答メッセージ送信制御部４４に通知する。

認証データ生成部４２は、ランダムチャレンジ受信制御部４１から供給されたランダムチャレンジに対して、送信側の端末１１（送信可否判定部２１の期待値生成部３３）における場合と同様の鍵付きハッシュ処理を施して、第三者が予測できない認証データを生成し、応答メッセージ生成部４３に供給する。

応答メッセージ生成部４３は、応答メッセージ送信制御部４４の制御に従って、認証データ生成部４２から供給された認証データを組み込んだ応答メッセージを生成し、応答メッセージ送信制御部４４に供給する。

応答メッセージ送信制御部４４は、通信部２３を介して、送信側の端末１１か

ら送信されてきた応答要求コマンドを受信する。

応答メッセージ送信制御部４４は、応答要求コマンドを受信する前のタイミングで（送信側の端末１１から応答要求コマンドが送信されてくる前のタイミングで)、応答メッセージ生成部４３を制御して、受信する応答要求コマンドに対応した認証データが組み込まれた応答メッセージを生成させるとともに、応答要求コマンドを受信したとき、通信部２３を介して、その応答メッセージを送信先の端末１１に送信する。

次に、図５のフローチャートを参照して、送信可否判定処理を行う場合の端末１１の送信可否判定部２１（図２，３）の動作を説明する。

ステップＳ１において、端末１１（送信側の端末１１）の送信可否判定部２１のランダムチャレンジ生成部３１は、ランダムチャレンジを生成し、それをランダムチャレンジ送信制御部３２および期待値生成部３３に供給する。

ステップＳ２において、ランダムチャレンジ送信制御部３２は、供給されたランダムチャレンジを、通信部２３を介して受信側の端末１１に送信し、ステップＳ３において、期待値生成部３３は、供給されたランダムチャレンジに対して鍵付きハッシュ処理を施して、受信側の端末１１で生成される認証データの期待値を生成する。

なおこの例の場合、送信側の端末１１は、データ送信の可否を判定するのに、最大Ｎ（＝１，２，・・・）回応答要求コマンドを送信するので、ここでは、送信され得るＮ個の応答要求コマンドに応じた認証データのＮ個の期待値が生成される。

Ｎ個の期待値は、例えば、ランダムチャレンジに対して鍵付きハッシュ処理を施した結果得られたデータを複数個に分割し、その分割して得られたデータからＮ個の期待値を生成することができる。図６の例の場合、ランダムチャレンジに対して鍵付きハッシュ処理を施した結果得られたデータが、Ｎ個に分割されて、Ｎ個の期待値１乃至期待値Ｎが生成される。

また、ランダムチャレンジに対する鍵付きハッシュ処理を、複数回繰り返して

行い、その処理毎に得られたデータから、Ｎ個の期待値を生成することができる。図７の例の場合、ランダムチャレンジに対する鍵付きハッシュ処理がＮ回繰り返して行われ、その処理毎に得られたＮ個のデータが期待値となる。図７中、期待値１は、ランダムチャレンジに鍵付きハッシュ処理が１回施された結果得られたものであり、期待値２は、期待値１に、鍵付きハッシュ処理がさらに施された結果得られたものである。

図５に戻り、ステップＳ４において、ランダムチャレンジ送信制御部３２は、後述するように受信側の端末１１から送信されてきた、ステップＳ２で送信されたランダムチャレンジを受信した旨を示すＲＣ受信メッセージを（ステップＳ２３）、通信部２３を介して受信し、その旨をコマンド送信制御部３４に通知する。ステップＳ５において、コマンド送信制御部３４は、応答要求コマンドが何番目に送信されるものか（送信の順番）を示すカウンタｉに１を初期設定する。

次に、ステップＳ６において、コマンド送信制御部３４は、通信部２３を介して、応答要求コマンドを受信側の端末１１に送信し、ステップＳ７において、応答時間計測部３６を制御して、応答時間の計測を開始させる。

ステップＳ８において、コマンド送信制御部３４は、後述するように受信側の端末１１から送信されてきた、ステップＳ６で送信された応答要求コマンドに対する応答しての応答メッセージを、通信部２３を介して受信して、判定部３５に供給し、ステップＳ９において、応答時間計測部３６を制御して、応答時間の計測を終了させる。すなわちステップＳ７で開始しステップＳ９で終了する時間計測で得られた時間が受信側の端末１１の応答時間となる。

ステップＳ１０において、判定部３５は、コマンド送信制御部３４から供給された応答メッセージに組み込まれている認証データと、期待値生成部３３により生成された、その認証データの期待値（具体的には、カウンタｉが示す順番に送信された応答要求コマンド（以下、第ｉ番目に送信された応答要求コマンドと称する）に対応する期待値）とが一致するか否かを判定し、一致すると判定した場合、受信側の端末１１を、情報通信システムにおける正規の端末であると認証し、

ステップＳ１１に進む。

ステップＳ１１において、判定部３５は、応答時間計測部３で計測された、第ｉ番目に送信された応答要求コマンドに対する受信側の端末１１の応答時間が所定の時間 TL を越えているか否かを判定する。時間 TL は、例えば、同一 LAN１に接続された端末１１間で要する通信時間である。すなわち応答時間が時間 TL を越える場合、受信側の端末１１は、送信側の端末１１と異なる LAN１に接続され、また、時間 TL を越えない場合（応答時間＝時間 TL を含む）、同一の LAN１に接続されていると判定することができる（通信距離を判別することができる）。

ステップＳ１１で、時間 TL を越えると判定された場合、ステップＳ１２に進み、判定部３５は、その結果を、コマンド送信制御部３４に通知し、コマンド送信制御部３４はそのとき、カウンタｉを１だけインクリメントする。

ステップＳ１３において、コマンド送信制御部３４は、カウンタ ｉ＝Ｎ＋１であるか否かを判定する。カウンタ ｉ＝Ｎ＋１ではないと判定された場合には、所定時間経過後、ステップＳ６に戻る。ステップＳ１３で、カウンタ ｉ＝Ｎ＋１であると判定されたとき（すなわち、応答要求コマンドの送信がＮ回行われたとき）、またはステップＳ１０で、受信側の端末１１が本情報通信システムにおける正規の機器ではないと判定されたとき、ステップＳ１４に進み、その旨を、判定部３５に通知する。判定部３５はそのとき、受信側の端末１１へのデータ送信を不可とし、通信部２３を制御して、送信データ格納部２４に格納されているデータの受信側の端末１１に対する送信を禁止する。

ステップＳ１１で、第ｉ番目に送信された応答要求コマンドに対する応答時間が、時間 TL を越えないと判定された場合、すなわち、受信側の端末１１が、本情報通信システムにおける正規の機器であり、かつ、例えば送信側の端末１１と同じ LAN１に接続されている端末１１であるとき、ステップＳ１５に進み、判定部３５は、通信部２３を制御して、送信データ格納部２４に格納されているデータを、受信側の端末１１に送信させる。

ステップＳ１４またはステップＳ１５で、受信側の端末１１に対するデータ送

信可否が判定されたとき、判定部３５は、通信部２３を介して、送信可否判定が終了した旨を表すメッセージ（以下、判定終了メッセージと称する）を受信側の端末１１に送信する。その後、送信可否判定処理は、処理を終了する。

次に、図５のフローチャートを参照して、応答処理を行う場合の端末１１の応答制御部２２（図２，４）の動作を説明する。

ステップＳ２１において、端末１１（受信側の端末１１）の応答制御部２２のランダムチャレンジ受信制御部４１は、送信先の端末１１から送信されてきたランダムチャレンジを（ステップＳ２）、通信部２３を介して受信し、認証データ生成部４２に供給する。ステップＳ２２において、認証データ生成部４２は、ランダムチャレンジ受信制御部４１から供給されたランダムチャレンジに対して、送信側の端末１１の送信可否判定部２１（期待値生成部３３）における鍵付きハッシュ処理（ステップＳ３）と同様の鍵付きハッシュ処理を施し、認証データを生成し、応答メッセージ生成部４３に供給する。

なおこの例では、最大Ｎ個の応答要求コマンドを受信し得るので、その応答要求コマンドに対応する期待値と対比される（ステップＳ１０）Ｎ個の認証データが生成される。Ｎ個の認証データは、期待値の生成方法（図６，７）と同じ方法で生成される。

このように認証データが生成されると、ステップＳ２３において、ランダムチャレンジ受信制御部４１は、通信部２３を介して、ＲＣ受信メッセージを送信側の端末１１に送信し、その旨を、応答メッセージ送信制御部４４に通知する。

ステップＳ２４において、応答メッセージ送信制御部４４は、これから受信する応答要求コマンドが何番目に受信されるものかを示すカウンタｊに１を初期設定し、ステップＳ２５において、応答メッセージ生成部４３を制御して、カウンタｊが示す順番に受信される応答要求コマンド（以下、第ｊ番目に受信される応答要求コマンドと称する）に対応する認証データを組み込んだ応答メッセージを生成させる。

次に、ステップＳ２６において、応答メッセージ送信制御部４４は、送信先の

端末１１から送信されてきた応答要求コマンドを（ステップＳ６）、通信部２３を介して受信すると、ステップＳ２７において、ステップＳ２５で生成された第ｊ番目に受信される応答要求コマンドに応じた認証データが組み込まれた応答メッセージを、通信部２３を介して、送信側の端末１１に送信する。これにより上述したように送信側の端末１１で（ステップＳ１０で）、第ｊ番目に受信された（第ｉ番目に送信された）応答要求コマンドに対応する認証データと、第ｉ番目に送信された（第ｊ番目に受信された）応答要求コマンドの期待値とが比較される。

ステップＳ２８において、受信側の端末１１の応答制御部２２の応答メッセージ送信制御部４４は、送信側の端末１１から送信される判定終了メッセージ（ステップＳ１６）が受信されたか否かを判定し、所定の時間内に受信されていないと判定した場合、ステップＳ２９に進む。ステップＳ２９において、応答メッセージ送信制御部４４は、カウンタｊを１だけインクリメントし、ステップＳ３０で、カウンタｊ＝Ｎ＋１であるか否かを判定する。

ステップＳ３０で、カウンタｊ＝Ｎ＋１ではないと判定されたとき（すなわち、応答要求コマンドをＮ回受信されていないとき）、ステップＳ２５に戻り、次に受信される応答要求コマンドに対して、それ以降の処理を実行する。

ステップＳ２８で、判定終了メッセージが受信されたとき、またはステップＳ３０で、カウンタｊ＝Ｎ＋１であると判定されたとき（すなわち、応答要求コマンドがＮ回受信されたとき）、応答制御部２２は、応答処理を終了する。

以上のように、ランダムチャレンジから生成された認証データ（ステップＳ２２）とその期待値（ステップＳ３）とに基づいて認証された受信側の端末１１についてのみ応答時間に基づく通信距離の判別を行うようにしたので（ステップＳ１０でＮＯの判定がなされた場合、ステップＳ１１の処理がスキップされるので）、正規の機器のようになりすました機器にデータが送信されることを防止することができる（正規の機器のようになりすました機器が応答要求コマンドを受信し、応答要求メッセージを送信して、その機器にデータが送信されることはない）。

また送信側の端末１１で、応答要求コマンドに、新たに生成したランダムチャ

レンジを込み込んで受信側の端末１１に送信し（ステップＳ６）、受信側の端末１１で、応答要求コマンドを受信したとき（ステップＳ２６）、予め生成された認証データ（ステップＳ２２）と、その応答要求コマンドに組み込まれたランダムチャレンジとを連結して、または両者の論理演算を行って新たな認証データを生成し、それを組み込んだ応答メッセージを返信することもできる（ステップＳ２７）。なおこのとき送信側の端末１１では、ステップＳ１０で新たな認証データと比較される期待値が、ステップＳ３で生成された期待値と、応答要求コマンドに組み込まれたランダムチャレンジと連結されて、または両者の論理演算が行われて生成される。

このように応答要求コマンドに組み込んだランダムチャレンジを利用して認証データおよび期待値が生成されるようにすることで、受信側の端末１１は、送信側の端末１１からの応答要求コマンドを受信した後でなければ、応答メッセージを送信することができなくなる。したがって、応答時間を短縮するために、応答要求コマンドを受信する前に応答メッセージを送信するなどといった不正行為を防止することができる。

また、以上のように、受信側の端末１１において、応答要求コマンドを受信する前に、認証データおよびそれが組み込まれた応答メッセージを生成するようにしたので（ステップＳ２２，Ｓ２５）、応答要求コマンドを受信した後直ちに応答メッセージを送信側の端末１１に返信することができる（ステップＳ２７）。

例えば、応答要求コマンドを受信した後に、認証データおよび応答要求メッセージを生成するようになされている場合、送信側の端末１１で計測される応答時間に、その処理にかかる時間が含まれてしまうので、通信時間としての応答時間を正確に計測することができない。しかしながら本発明のように応答要求コマンドを受信した後直ちに応答メッセージを送信することができるようにしておくことにより、通信時間としての応答時間が正確に計測される。

また、以上においては、送信側の端末１１がランダムチャレンジを生成し（ステップＳ１）、受信側の端末１１に提供するようにしたが（ステップＳ２）、受信

側の端末１１が生成して送信側の端末１１に提供するようにすることもできる。

また、以上においては、秘密鍵を送信側の端末１１と受信側の端末１１で共有している場合を例として説明したが、秘密鍵の共有がない場合には、デフィー・ヘルマン鍵交換（Diffie-Hellman key exchange）のアルゴリズムなどを使って鍵の共有を行うことができる。この場合は、鍵交換した相手は、応答時間を測定する相手であることの証明書などを基に確認される。鍵交換の後、鍵交換で得られた鍵そのものを認証データと期待値とすることもできるし、上記のように乱数に交換した鍵での鍵付きハッシュ処理を施し、認証データや期待値を得るようにすることもできる。

また以上においては、送信側の端末１１において、受信側の端末１１で生成された応答の認証データ（以下、認証データ RR と称する）（ステップＳ２２）と送信側の端末１１で生成された応答の期待値（以下、期待値 QR と称する）（ステップＳ３）とに基づき受信側の端末１１が認証されたが（ステップＳ１０）、受信側の端末１１においても、送信側の端末１１からの応答要求コマンドの認証データ（以下、認証データ RS と称する）とその期待値（以下、期待値 QS と称する）とに基づき送信側の端末１１の認証を行うようにすることができる。

図５の例では、受信側の端末１１は、応答要求コマンドを受ければ（ステップＳ２６）、直ちに応答メッセージを送り返すので（ステップＳ２７）、例えば、図８に示すように、送信側の端末１１（送信機器）と同一の LAN１に第３の機器ｘを挿入し、はじめに機器ｘが受信機器に応答要求コマンドを送って（Ｓ１１１）、受信機器から応答メッセージを取得しておき（Ｓ１１２）、そして送信機器から応答要求コマンドが来たときに（Ｓ１２１）、取得した応答メッセージを返すことで（Ｓ１２２）、機器ｘは、正規の機器になりすますことができる。

そこで受信側の端末１１においても、応答メッセージを返信する際に、送信側の端末１１を認証すれば、このような不正を防止することができる（不正な機器に応答メッセージを返信することを防止することができる）。

図９は、送信可否判定部２１の、図１０は、応答制御部２２の、このように受

信側の端末１１でも送信側の端末１１の認証がなされる場合の構成例を示している。

送信可否判定部２１のランダムチャレンジ生成部５１は、図３のランダムチャレンジ生成部３１と同様に、所定ビット数の疑似乱数列を、ランダムチャレンジRCとして生成し、期待値生成部５２および認証データ生成部５３に供給する。

期待値生成部５２は、ランダムチャレンジ生成部５１から供給されたランダムチャレンジRCに対して、例えば、受信側の端末１１と共有する秘密鍵を利用した受信側の端末１１（認証データ生成部７３）における場合と同様の鍵付きハッシュ処理を施して、受信側の端末１１の認証データRRの期待値QR（対応する認証データRRと同値の期待値QR）を生成し、応答認証部５７に供給する。

認証データ生成部５３は、ランダムチャレンジ生成部５１から供給されたランダムチャレンジRCに対して、受信側の端末１１と共有する秘密鍵を利用した鍵付きハッシュ処理を施して、第三者が予測できないコマンドの認証データRSを生成し、応答要求コマンド送信部５５に供給する。

制御コマンド通信制御部５４は、開始コマンド等の制御コマンドCCを受信側の端末１１に送信したり、受信側の端末１１から送信されてきた、制御コマンドCCに対する応答メッセージCCRを受信する。

応答要求コマンド送信部５５は、認証データ生成部５３により生成された認証データRSを含む、応答要求コマンドMCを、通信部２３を介して、受信側の端末１１に送信する。

応答受信部５６は、送信された応答要求コマンドMCに対する応答として、受信側の端末１１から送信されてきた応答メッセージMCRを、通信部２３を介して受信し、そこに組み込まれている応答の認証データRRを応答認証部５７に供給する。

応答認証部５７は、応答受信部５６からの応答の認証データRRと、期待値生成部５２で生成されたその認証データRRの期待値QRに基づいて、受信側の端末１１が、本情報通信システムにおける正規の機器であるかの認証を行い、その認証結果を、制御判定部５８に通知する。

制御判定部５８は、応答時間計測部５９で計測された、応答要求コマンドMCに対する受信側の端末１１の応答時間RTTが所定の時間TLを越えているか否かを判定して、通信距離の判別（送信側の端末１１と同一のLAN1に接続されているかの判定）を行う。

制御判定部５８は、受信側の端末１１の認証結果および通信距離の判別結果に基づいて、受信側の端末１１に対するデータの送信可否の判定を行う。制御判定部５８は、その判定結果に基づいて、通信部２３を制御し、送信データ格納部２４に格納されているデータを、受信側の端末１１に送信させる。

応答時間計測部５９は、応答要求コマンド送信部５５および応答受信部５６からの通知に応じて、応答要求コマンドMCに対する、受信側の端末１１の応答時間RTTを計測する。

次に、応答制御部２２の構成（図１０）を説明する。

制御応答通信制御部７１は、通信部２３を介して、送信側の端末１１から送信されてきた制御コマンドCCを受信したり、その制御コマンドCCに対する応答メッセージCCRを送信側の端末１１に送信する。

期待値生成部７２は、制御応答通信制御部７１により受信された制御コマンドCCに含まれるランダムチャレンジRCに対して、送信側の端末１１と共有する秘密鍵を利用した送信側の端末１１（認証データ生成部５３）における場合と同様の鍵付きハッシュ処理を施して、送信側の端末１１のコマンド認証データRSの期待値QS（対応する認証データRSと同値の期待値QS）を生成し、コマンド認証部７６に供給する。

認証データ生成部７３は、制御応答通信制御部７１により受信された制御コマンドCCに含まれるランダムチャレンジRCに対して、送信側の端末１１と共有する秘密鍵を利用した鍵付きハッシュ処理を施して、第三者が予測できない応答の認証データRRを生成し、応答送信部７４に供給する。

応答送信部７４は、コマンド認証部７６による認証結果に基づいて、認証データ生成部７３により生成された応答の認証データRRを含む、送信側の端末１１か

らの応答要求コマンドMCに対する応答メッセージMCRを、通信部２３を介して送信側の端末１１に送信する。

応答要求コマンド受信部７５は、送信側の端末１１から送信されてきた応答要求コマンドMCを、通信部２３を介して受信し、そこに組み込まれているコマンドの認証データRSをコマンド認証部７６に供給する。

コマンド認証部７６は、応答要求コマンド受信部７５からのコマンドの認証データRSと、期待値生成部７２で生成されたその認証データRSの期待値QSに基づいて、送信側の端末１１が、本情報通信システムにおける正規の機器であるかの認証を行い、その認証結果を、応答送信部７４に通知する。

次に、図９の送信可否判定部２１の動作を、図１１のフローチャートを参照して説明する。

ステップＳ５１において、端末１１の送信可否判定部２１の制御コマンド通信制御部５４は、受信側の機器と、TCPコネクションを確立する。TCPコネクションのためのポート番号は予め送信側の端末１１と受信側の機器の間で合意されているものとする。送信側の機器と受信側の機器の間で事前にTCPコネクションが確立している場合はこのステップを省略してよい。

制御コマンド通信制御部５４は、確立したTCPコネクションを介して、応答時間RTTの計測を開始する旨を表す開始コマンド（制御コマンドCC）を受信側の機器に送信する。この開始コマンドCCには、セッション番号SID、ランダムチャレンジRC、送信側の端末１１が実行可能な、１セッションでの応答時間RTTの計測のリトライ数（計測回数）ksが含まれている。

セッション番号SIDは、これから行われる受信側の機器に対する一連の認証処理（１つのセッション）に割り当てられた番号であり、この番号を送信側と受信側とで共有することにより、セッション毎に認証処理を区別することができる。

また応答時間RTTの計測のために必要なデータ（例えば、応答要求コマンドMCやその応答メッセージMCR）の通信は、パケットの再送を行わないUDPでなされるので、通信状態によっては、データが途中で消滅してしまうなど、応答時間RTT

の計測が適切に行われない場合も考えられる。またネットワーク内の他の通信の影響を受けて、パケットの伝送に遅延が生じることもある。そこで応答時間 RTT の計測を何回かリトライ（再施行）できるようになされている。このリトライの回数は、送信側の機器と受信側の機器の設定によって異なることもあるので、この例ではここで送信側の機器のリトライ数（例えば、最大のリトライ数）ks が受信側の機器に通知される。

次に、ステップＳ５２において、制御コマンド通信制御部５４は、開始コマンド CC に対する、受信側の機器からの応答メッセージ CCR を受信する。

この応答メッセージ CCR には、開始コマンド CC に含まれていたセッション番号 SID の他、受信側が決定した１セッションでの応答時間 RTT 計測のリトライ数 k、および応答要求コマンド MC を受信するための UDP ポート番号 pb が含まれている。すなわち開始コマンド CC とその応答メッセージ CCR の授受により、送信側の端末１１と受信側の機器は、応答時間 RTT の計測のリトライ数（計測回数）k とセッション番号 SID、および応答要求コマンド MC とその応答メッセージ MCR の授受のために利用する UDP ポート番号ｐｂを合意する。

なお受信側の機器は、開始コマンド CC を介して通知された送信側の端末１１で実行可能な応答時間 RTT 計測のリトライ数 ks と受信側が実行可能の応答時間 RTT 計測のリトライ数のうちの小さい方を、今回の応答時間 RTT 計測のリトライ数 k に決定し、応答メッセージ CCR を介して送信側の機器に通知する。

ステップＳ５３において、期待値生成部５２は、ランダムチャレンジ生成部５１により生成されたランダムチャレンジ RC に対して、受信側の端末１１の応答制御部２２（認証データ生成部７３）における鍵付きハッシュ処理と同様の鍵付きハッシュ処理を施し、受信側の機器の認証データ RR の期待値 QR を生成する。

この例の場合、応答時間 RTT 計測が最大 k 回行われるので（応答要求コマンド MC の応答メッセージ MCR が最大 k 回受信されるので）、受信され得る k 個の応答メッセージ MCR に含まれる認証データ RR それぞれの期待値 QR が生成される。

またこのとき認証データ生成部５３は、ランダムチャレンジ生成部５１により

生成されたランダムチャレンジRCに対して鍵付きハッシュ処理を施して、コマンドの認証データRSを生成する。

この例の場合、応答時間RTT計測が最大k回行われるので（応答要求コマンドMCが最大k回送信されるので）、送信され得るk個の応答要求コマンドMCそれぞれの認証データRSが生成される。

ステップＳ５４において、制御判定部５８に内蔵されるカウンタｉの値が１に初期設定される。このとき期待値生成部５２は、カウンタｉの値に対応する期待値QR（例えば、第ｉ番目に生成された期待値QRi）を応答認証部５７に供給する。また認証データ生成部５３は、カウンタｉの値に対応する認証データRSiを、応答要求コマンド送信部５５に供給する。

ステップＳ５５において、応答要求コマンド送信部５５は、セッション番号SID、認証データ生成部５３から供給された認証データRSi（k個の認証データRSのうちのカウンタｉの値に対応する認証データRSi）、およびシーケンス番号Ci（カウンタｉの値を表す番号）を含む応答要求コマンドMCを、制御コマンドCCの応答CCRに含まれていたUDPポート番号pbでのUDP通信で、受信側の機器に送信する。

応答要求コマンド送信部５５は、応答要求コマンドMCを送信したとき、その旨の通知STRを応答時間計測部５９に行う。これにより応答時間計測部５９は、応答時間の計測を開始する。

ステップＳ５６において、応答受信部５６は、受信側の機器からの応答メッセージMCRを受信したか否かを判定し、受信していないと判定した場合、ステップＳ５７に進み、所定時間以上応答を待っているか否かを判定する（ステップＳ５５で応答時間RTT計測が開始されてから所定の時間経過したか否かを判定する）。

ステップＳ５７で、まだ所定の時間経過していないと判定された場合、ステップＳ５６に戻り、それ以降の処理が実行される。一方ステップＳ５７で所定の時間経過したと判定された場合、ステップＳ６２に進み、カウンタｉの値がリトライ数kより小さいか否かが判定され（応答時間RTTの計測がk回行われたか否かが判定され）、小さいと判定された場合（k 回行われていない場合）、ステップＳ

６３に進み、カウンタｉの値が１だけインクリメントされて、ステップＳ５５に戻る。

応答要求コマンドMCを送るUDPでは、パケットが通信相手に届かないことがあるので、送信側の端末１１は、応答要求コマンドMCを送った後、所定時間が経っても応答メッセージMCRが受信されない場合は、この回の計測は失敗したものとして、次の応答時間RTTの計測が開始される（ステップＳ５５以降の処理が開始される）。

ステップＳ５６で、応答メッセージMCRが受信されたと判定された場合、ステップＳ５８に進み、応答受信部５６は、受信した応答メッセージMCRに含まれている応答の認証データRRj、およびシーケンス番号Cjを読み出し、応答認証部５７に供給する。

応答認証部５７は、応答受信部５６から供給されたシーケンス番号Cjが、カウンタｉの値（送信された応答要求コマンドMCのシーケンス番号Ci）と一致するか否かを判定する。

なお応答メッセージMCRのシーケンス番号Cjと応答要求コマンドMCのシーケンス番号Ciを確認することの効果については後述する。

ステップＳ５８で、一致しないと判定された場合、ステップＳ５６に戻り、それ以降の処理が行われ、一致すると判定された場合、ステップＳ５９に進む。

ステップＳ５９において、応答受信部５６は、応答メッセージMCRを受信した旨の通知ENDを応答時間計測部５９に行う。応答時間計測部５９は、ステップＳ５５で開始した応答時間RTT計測を終了し、計測結果（応答時間RTT）を、制御判定部５８に供給する。

ステップＳ６０において、応答認証部５７は、応答受信部５６から供給された応答の認証データRRjと、期待値生成部５２により生成された、その認証データRRjの期待値QRiとが一致するか否かを判定し、一致すると判定した場合、受信側の端末１１を、本情報通信システムにおける正規の端末であると認証し、ステップＳ６１に進む。

ステップＳ６１において、制御判定部５８は、応答時間計測部５９から供給された応答時間 RTT が、所定の規定時間ＴＬより大きいか否かを判定する。

規定時間ＴＬは、応答時間 RTT が、送信側の端末１１と受信側の機器が同一 LAN１に接続されていたならば、それを超えないであろう時間である。すなわち応答時間 RTT が規定時間ＴＬより大きければ、受信側の機器は送信側の端末１１と同一の LAN１に接続されていないと判定することができる。一方、応答時間 RTT が規定時間ＴＬより大きくない（それ以下である場合）、受信側の機器は送信側の端末１１と同一 LAN１に接続されていると判定することができる。

ステップＳ６１で、YES の判定がなされたとき（第ｉ回目の応答時間 RTT 計測で、受信側の機器が送信側の端末１１と同一の LAN１に接続されているものではないと判定されたとき）、ステップＳ６２に進み、制御判定部５８は、カウンタｉの値がｋより小さい値か否か（応答時間 RTT 計測がｋ回リトライされたか否か）を判定し、小さいと判定した場合（応答時間 RTT 計測がまだｋ回行われていない場合）、ステップＳ６３に進み、カウンタｉの値が１だけインクリメントされる。このとき期待値生成部５２は、カウンタｉの新たな値に対応する期待値 QRi を応答認証部５７に供給し、認証データ生成部５３は、カウンタｉの新たな値に対応する認証データ RSi を、応答要求コマンド送信部５５に供給する。

その後ステップＳ５５に戻り、それ以降の処理が行われる。すなわち応答時間 RTT が規定時間ＴＬ内になる応答メッセージ MCR が得られるまで、最大ｋ回、応答時間 RTT の計測が行われる。

ステップＳ６１で、NO の判定がなされたとき（応答時間 RTT が規定時間ＴＬ以下となる応答メッセージ MCR が得られたとき）、ステップＳ６４に進む。

ステップＳ６４に進み、制御判定部５８は、受信側の機器は、送信データを送信できる機器（正規の機器であって、送信側の端末１１と同じ LAN１に接続されている機器）である旨を、通信部２３（図３）に通知する。これにより通信部２３は、所定の送信データを送信データ格納部２４から読み出して、受信側の機器（端末１１）に送信する。

ステップＳ６２で、カウンタｉの値が、ｋ以上であると判定された場合（応答時間 RTT の計測をｋ回行っても、応答時間 RTT が規定時間ＴＬ以下になる応答が得られなかった場合)、ステップＳ６５に進み、制御判定部５８は、受信側の機器は、ローカルネットワーク外の機器（送信側の端末１１と同じ LAN１に接続されていない機器）である旨を、制御コマンド通信制御部５４に通知する。これにより制御コマンド通信制御部５４は、受信側の機器の認証が失敗した旨を示す終了コマンド CC を、受信側の機器に送信する。

ステップＳ６０で、応答の認証データ RRj とその期待値 QRi 一致しないと判定された場合、ステップＳ６６に進み、制御判定部５８は、受信側の機器は、不正な機器である旨を、制御コマンド通信制御部５４に通知する。これにより制御コマンド通信制御部５４は、受信側の機器の認証が失敗した旨を示す終了コマンド CC を、受信側の機器に送信する。

以上のようにして送信可否判定処理が行われる。

なお以上においては、ステップＳ５３においてｋ個の認証データ RS を生成したが、それに代えて、ステップＳ５５において、応答要求コマンド MC を送信する毎にそのコマンドに使う認証データ RS を毎回生成するようにしてもよい。

次に、図１０の応答制御部２２の動作を、図１２のフローチャートを参照して説明する。

ステップＳ８１において、受信側の端末１１の応答制御部２２の制御応答通信制御部７１は、送信側の機器と協働して、TCP コネクションを確立し、その TCP コネクションを介して送信側の機器から送信されてきた、開始コマンド CC（ステップＳ５１）を受信する。制御応答通信制御部７１は、受信した開始コマンド CC に含まれているランダムチャレンジ RC を、期待値生成部７２および認証データ生成部７３に供給する。

次にステップＳ８２において、応答要求コマンド受信部７５は、送信側の機器から送信されてくる応答要求コマンド MC を受信するための UDP ポート番号 pb を決定する。

応答要求コマンド受信部７５はまた、制御コマンドCCに含まれている送信側の機器が実行可能な応答時間RTT計測のリトライ数ksと、受信側の端末１１が対応可能な応答時間RTTの計測のリトライ数のいずれか小さい方を、今回の応答時間RTTの計測のリトライ数kに決定する。

ステップＳ８３において、制御応答通信制御部７１は、ステップＳ８１で受信された制御コマンドCCに含まれていたセッション番号SID、応答時間RTTの計測のリトライ数k、およびUDPポート番号pbを含む応答メッセージCCRを、ステップＳ８１で確立されたTCPコネクトを介して送信側の機器に送信する。送信側の機器は、ここで送信された応答メッセージCCRを受信する（ステップＳ５２）。

ステップＳ８４において、認証データ生成部７３は、制御応答通信制御部７１から供給されたランダムチャレンジRCに対して鍵付きハッシュ処理を施して、応答の認証データRRを生成する。

この例の場合、応答時間RTT計測が最大k回行われるので（応答要求コマンドMCの応答メッセージMCRが最大k回送信されるので）、送信され得るk個の応答メッセージMCRそれぞれの認証データRRが生成される。

期待値生成部７２は、制御応答通信制御部７１から供給されたランダムチャレンジRCに対して、送信側の端末１１の送信可否判定部２１（認証データ生成部５３）における鍵付きハッシュ処理と同様の鍵付きハッシュ処理を施し、送信側の端末１１の認証データRSの期待値QSを生成する。

この例の場合、応答時間RTT計測が最大k回行われるので（応答要求コマンドMCが最大k回受信されるので）、受信され得るk個の応答要求コマンドMCに含まれる認証データRSそれぞれの期待値QSが生成される。

ステップＳ８５において、コマンド認証部７６に内蔵されているカウンタjの値が１に初期設定される。

ステップＳ８６において、コマンドが受信されるまで待機され、コマンドが受信されたと判定された場合、ステップＳ８７に進み、受信されたコマンドが応答要求コマンドMC（ステップＳ５５）であるか否かを判定し、応答要求コマンドMC

であると判定された場合、ステップＳ８８に進む。

ステップＳ８８において、受信されたコマンドに含まれるシーケンス番号 Ci とカウンタｊが比較され、シーケンス番号 Ci がカウンタｊ以上の値であることが確認される。カウンタｊ以上の値である場合、ステップＳ８９に進み、カウンタｊがシーケンス番号 Ci の値に設定される。

これは、コマンドが欠落した場合、順番どおりに来なかった場合に、カウンタｊをシーケンス番号 Ci に合致させるための対策である。

期待値生成部７２はこのとき、カウンタｊの値に対応する期待値 QS（例えば、第ｊ番目に生成された期待値 QSj）をコマンド認証部７６に供給する。また認証データ生成部７３は、カウンタｊの値に対応する認証データ RRj を、応答送信部７４に供給する。

次にステップＳ９０において、コマンド認証部７６は、応答要求コマンド受信部７５により受信された応答要求コマンド MC に組み込まれている認証データ RSi と、期待値生成部７２により生成された期待値 QSj（カウンタｊが示す順番に生成された期待値）とが一致するか否かを判定し、一致すると判定した場合、送信側の端末１１を、本情報通信システムにおける正規の端末であると認証し、ステップＳ９１に進む。

ステップＳ９１において、コマンド認証部７６は、送信側の端末１１が正規の機器である旨を、応答送信部７４に通知する。これにより応答送信部７４は、セッション番号 SID、カウンタｊの値を表すシーケンス番号 Cj、認証データ生成部７３から供給された認証データ RRj を含む応答メッセージ MCR を、送信側の機器に送信する。

一方ステップＳ９０で、一致しないと判定された場合、ステップＳ９２に進み、コマンド認証部７６は、その旨を、応答送信部７４に通知する。これにより応答送信部７４は、セッション番号 SID、カウンタｊの値を表すシーケンス番号 Cj、および送信側の機器における受信側の機器の認証（ステップＳ６０）が失敗するような認証データ RR（＝××）を含む応答メッセージ MCR を、送信側の機器に送

信する。

ステップＳ９１またはステップＳ９２で、応答メッセージMCRが送信されたとき、ステップＳ９３で、カウンタｊの値が１だけインクリメントされ、その後、ステップＳ８６に戻り、それ以降の処理が実行される。

また、ステップＳ８８において、カウンタｊの値が受信されたコマンドに含まれるシーケンス番号Ciよりも小さい場合も、ステップＳ８６に戻り、それ以降の処理が実行される。

ステップＳ８７で、受信されたコマンドが応答要求コマンドではないと判定された場合（終了コマンド CC（ステップＳ６５，Ｓ６６）であるとき)、処理は終了する。

次に図１１のステップＳ５８の処理について説明する。ステップＳ５８の処理では、受信側の機器からの応答メッセージMCRのシーケンス番号Cjと応答要求コマンドMCのシーケンス番号Ci（カウンタｉの値）が一致するか否かが判定されるが、このように応答要求コマンドMCと応答メッセージMCRの対応関係を確認するようにしたので、応答要求コマンドMCに対応しない応答メッセージMCR（他の応答要求コマンドMCの応答メッセージMCR）に基づいて応答時間RTTによる距離判定が行われない。

例えば、図１３に示すように、受信側の機器で、第１番目の応答要求コマンドMCに対する応答メッセージMCRの送信に時間がかかり（ステップＳ９１，Ｓ９２)、送信側の端末１１で、タイムアウトと判定されて（ステップＳ５７)、第２番目の応答要求コマンドMCが受信側の機器に送信されたものとする。第１番目の応答要求コマンドMCに対する応答メッセージMCRは、第２番目の応答要求コマンドMCが送信された後（ステップＳ５５)、第２番目の応答要求コマンドMCとの関係でタイムアウトとならない間（ステップＳ５７）に送信側の端末１１に受信されたものとする（ステップＳ５６)。

しかしながらこの場合本発明では、受信側の機器からの第１番目の応答メッセージMCRのシーケンス番号（＝１）と、第２番目の応答要求コマンドMCのシーケ

ンス番号（＝２）が一致しないと判定され、送信側の端末１１は、第２番目の応答要求コマンドMCに対する応答メッセージMCRが受信されるまで待機することになり（ステップＳ５６に戻る）、対応しない応答メッセージMCRが受信されても応答時間RTTによる距離判定は行われない。

次に、不正に対する端末１１の動作を具体的に説明する。

例えば図８に示した送信機器と同一のLAN１に接続された不正な機器ｘが、受信機器から応答を得るために応答要求コマンドを送信するものとする。しかしながら、機器ｘは、受信機器と共有する秘密鍵を有していないので、受信機器での送信機器の認証に必要な認証データRSを得ることができない。したがって図１４に示すように、機器ｘが、不適当な認証データRS（＝？）を含む応答要求コマンドMCを受信機器に送信するが、受信機器からは、受信機器の認証が失敗する認証データRR（＝××）を含む応答メッセージMCRが送信されてくる（ステップＳ９２）。したがって機器ｘが、その後、送信機器からの応答要求コマンドMCに対して、その応答メッセージMCRを送信機器に送信して応答しても、送信機器において、機器ｘは認証されず、送信データは機器ｘに送信されない。

そこで図１５に示すように、不正の機器ｘは、送信機器から応答要求コマンドMCを受けてそれを受信機器に送信し、受信機器から、適当な認証データRRを含む応答メッセージMCRを取得する。そして機器ｘは、取得した応答メッセージMCRを、送信機器に送信することも考えられる。

しかしながらこの例の場合、応答要求コマンドMCは、送信機器から機器ｘ、そして機器ｘから受信機器に送信され、応答メッセージMCRが、受信機器から機器ｘに、そして機器ｘから送信機器へ伝送されるので、応答要求コマンドMCと応答メッセージMCRの伝送路が、通常の伝送経路（送信機器と受信機器間の伝送路）より長くなる。したがってこの場合、結局応答時間RTTが規定時間TLより長くなるので、機器ｘは、送信機器と同一 LAN１に接続されていないものとして、機器ｘには送信データが提供されない。

上述した一連の処理は、ハードウエアにより実現させることもできるが、ソフ

トウエアにより実現させることもできる。一連の処理をソフトウエアにより実現する場合には、そのソフトウエアを構成するプログラムがコンピュータにインストールされ、そのプログラムがコンピュータで実行されることより、上述した送信可否判定部２１および応答制御部２２が機能的に実現される。

図１６は、上述のような送信可否判定部２１および応答制御部２２として機能するコンピュータ１０１の一実施の形態の構成を示すブロック図である。CPU（Central Processing Unit）１１１にはバス１１５を介して入出力インタフェース１１６が接続されており、CPU１１１は、入出力インタフェース１１６を介して、ユーザから、キーボード、マウスなどよりなる入力部１１７から指令が入力されると、例えば、ROM（Read Only Memory）１１２、ハードディスク１１４、またはドライブ１２０に装着される磁気ディスク１３１、光ディスク１３２、光磁気ディスク１３３、若しくは半導体メモリ１３４などの記録媒体に格納されているプログラムを、RAM（Random Access Memory）１１３にロードして実行する。これにより、上述した各種の処理が行われる。さらに、CPU１１１は、その処理結果を、例えば、入出力インタフェース１１６を介して、LCD（Liquid Crystal Display）などよりなる出力部１１８に必要に応じて出力する。なお、プログラムは、ハードディスク１１４やROM１１２に予め記憶しておき、コンピュータ１０１と一体的にユーザに提供したり、磁気ディスク１３１、光ディスク１３２、光磁気ディスク１３３，半導体メモリ１３４等のパッケージメディアとして提供したり、衛星、ネットワーク等から通信部１１９を介してハードディスク１１４に提供することができる。

なお、本明細書において、記録媒体により提供されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

産業上の利用可能性

第１および第３の本発明によれば、受信装置の応答時間を適切に計測することができる。

第２および第４の本発明によれば、送信装置における応答時間の適切な計測に必要な情報を提供することができる。

請求の範囲

1． 受信装置との間で共有する共有データに基づいて認証データが生成された後、応答を要求するコマンドを前記受信装置に送信するコマンド送信手段と、

前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づいて前記受信装置を認証する認証手段と、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測手段と、

前記認証手段による認証結果、および前記計測手段により計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定手段と

を備えることを特徴とする情報処理装置。

2． 前記コマンド送信手段は、データの送信可否を判定するのに、前記コマンドを最大N回送信し、

前記認証手段は、前記コマンドの送信の順番に応じた前記認証データとその前記期待値とに基づいて、前記受信装置を認証する

ことを特徴とする請求の範囲第1項に記載の情報処理装置。

3． 受信装置との間で共有する共有データに基づいて認証データが生成された後、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、

前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づいて前記受信装置を認証する認証ステップと、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップと、

前記認証ステップでの認証結果、および前記計測ステップの処理で計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと

を含むことを特徴とする情報処理方法。

4． 受信装置との間で共有する共有データに基づいて認証データが生成された後の、応答を要求するコマンドの前記受信装置に対する送信を制御するコマンド送信制御ステップと、

前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づく前記受信装置の認証を制御する認証制御ステップと、

前記受信装置からの、前記コマンドに対する応答時間の計測を制御する計測制御ステップと、

前記認証制御ステップでの認証結果、および前記計測制御ステップの処理で計測された応答時間に基づく、前記受信装置に対するデータの送信可否の判定を制御する判定制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

5．　受信装置との間で共有する共有データに基づいて認証データが生成された後の、応答を要求するコマンドの前記受信装置に対する送信を制御するコマンド送信制御ステップと、

前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づく前記受信装置の認証を制御する認証制御ステップと、

前記受信装置からの、前記コマンドに対する応答時間の計測を制御する計測制御ステップと、

前記認証制御ステップでの認証結果、および前記計測制御ステップの処理で計測された応答時間に基づく、前記受信装置に対するデータの送信可否の判定を制御する判定制御ステップと

を含む処理をコンピュータに実行させることを特徴とするプログラム。

6．　送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置において、

前記送信装置から前記コマンドが送信されてくる前に、前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成手段と、

前記送信装置から前記コマンドが送信されてくる前に、前記認証データ生成手段により生成された前記認証データを含む、前記コマンドに対する応答メッセー

ジを生成する応答メッセージ生成手段と、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信手段と

を備えることを特徴とする情報処理装置。

7． 前記共有データは、疑似乱数であり、

前記疑似乱数は、前記コマンドの前に前記送信装置から送信され、

前記認証データ生成手段は、前記疑似乱数に対して鍵付きハッシュ処理を施し、その結果得られたハッシュ値を前記認証データとする

ことを特徴とする請求の範囲第6項に記載の情報処理装置。

8． 前記認証データ生成手段は、前記疑似乱数と前記情報処理装置固有の情報に対して、鍵付きハッシュ処理を施し、その結果得られたハッシュ値を前記認証データとする

ことを特徴とする請求の範囲第7項に記載の情報処理装置。

9． データの送信可否を判定するのに、前記送信装置から、前記コマンドが最大N回送信されてくる場合において、

前記認証データ生成手段は、前記送信装置から最初の前記コマンドが送信されてくる前に、前記共有データに対して前記処理を施して、送信されてくるN個の前記コマンドのそれぞれに対応するN個の前記認証データを生成し、

前記送信手段は、N個の前記認証データが、前記送信装置と予め合意した順番で前記送信装置に提供されるように、前記応答メッセージ生成手段により生成された前記応答メッセージを前記送信装置に送信する

ことを特徴とする請求の範囲第6項に記載の情報処理装置。

10． 前記認証データ生成手段は、前記共有データに対して前記処理を施して得られたデータを複数個に分割し、分割されたデータからN個の前記認証データを生成する

ことを特徴とする請求の範囲第9項に記載の情報処理装置。

11．前記認証データ生成手段は、前記共有データに対して前記処理を繰り返し

施し、その処理毎に得られたデータから、Ｎ個の前記認証データを生成する

ことを特徴とする請求の範囲第９項に記載の情報処理装置。

１２．　前記送信手段は、前記送信装置からの前記コマンドが受信されたとき、前記認証データと前記コマンドに含まれる情報から生成された新たな認証データを含む応答メッセージを、前記送信装置に送信する

ことを特徴とする請求の範囲第６項に記載の情報処理装置。

１３．　送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置の情報処理方法において、

前記送信装置から前記コマンドが送信されてくる前に、前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成ステップと、

前記送信装置から前記コマンドが送信されてくる前に、前記認証データ生成ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信ステップと

を含むことを特徴とする情報処理方法。

１４．　送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信するためのプログラムであって、

前記送信装置から前記コマンドが送信されてくる前の、前記共有データに対して所定の処理を施しての前記認証データの生成を制御する認証データ生成制御ステップと、

前記送信装置から前記コマンドが送信されてくる前の、前記認証データ生成制御ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたときの、前記応答メッセージの前記送信装置に対する送信を制御する送信制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

１５．　送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信するためのプログラムであって、

前記送信装置から前記コマンドが送信されてくる前の、前記共有データに対して所定の処理を施しての前記認証データの生成を制御する認証データ生成制御ステップと、

前記送信装置から前記コマンドが送信されてくる前の、前記認証データ生成制御ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたときの、前記応答メッセージの前記送信装置に対する送信を制御する送信制御ステップと

を含む処理をコンピュータに実行させることを特徴とするプログラム。

１６．　受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成手段と、

前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信手段と、

前記コマンドに対する受信装置からの応答を受信する応答受信手段と

前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証手段と、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測手段と、

前記認証手段による認証結果、および前記計測手段により計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定手段と

を備えることを特徴とする情報処理装置。

１７．　前記コマンド送信手段は、データの送信可否を判定するのに、前記コマンドを最大ｋ回送信し、

前記認証手段は、前記コマンドの送信の順番に応じた前記認証データとその前記期待値とに基づいて、前記受信装置を認証する

ことを特徴とする請求の範囲第１６項に記載の情報処理装置。

１８．　受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、

前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、

前記コマンドに対する受信装置からの応答を受信する応答受信ステップと、

前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証ステップと、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップと、

前記認証ステップの処理での認証結果、および前記計測ステップにより計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと

を含むことを特徴とする情報処理方法。

１９．　受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、

前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、

前記コマンドに対する受信装置からの応答を受信する応答受信ステップと、

前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証ステップと、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップと、

前記認証ステップの処理での認証結果、および前記計測ステップにより計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

２０．　受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、

前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、

前記コマンドに対する受信装置からの応答を受信する応答受信ステップと、

前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証ステップと、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップと、

前記認証ステップの処理での認証結果、および前記計測ステップにより計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと

を含む処理をコンピュータに実行させることを特徴とするプログラム。

２１．　所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置において、

前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成手段と、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成手段により生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証手段と、

前記認証手段による認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信手段と

を備えることを特徴とする情報処理装置。

２２．　所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置の情報処理方法において、

前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成ステップの処理で生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証ステップと、

前記認証ステップの処理での認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信ステップと

を備えることを特徴とする情報処理方法。

２３．　所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置の情報処理用のプログラムであって、

前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成ステップの処理で生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証ステップと、

前記認証ステップの処理での認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録され

ている記録媒体。

２４．　所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置の情報処理用のプログラムであって、

前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成ステップの処理で生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証ステップと、

前記認証ステップの処理での認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信ステップと

を含む処理をコンピュータに実行させることを特徴とするプログラム。

図1

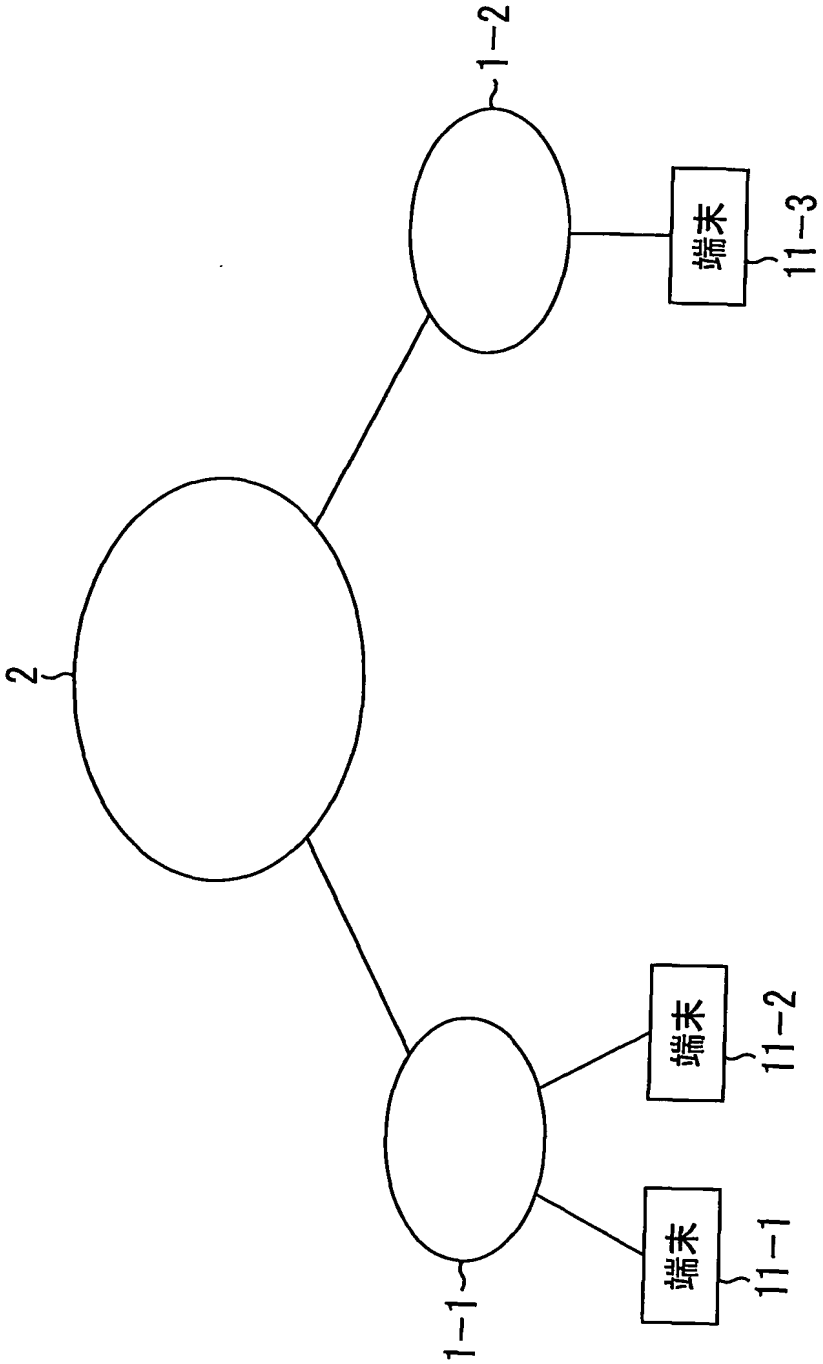


図2

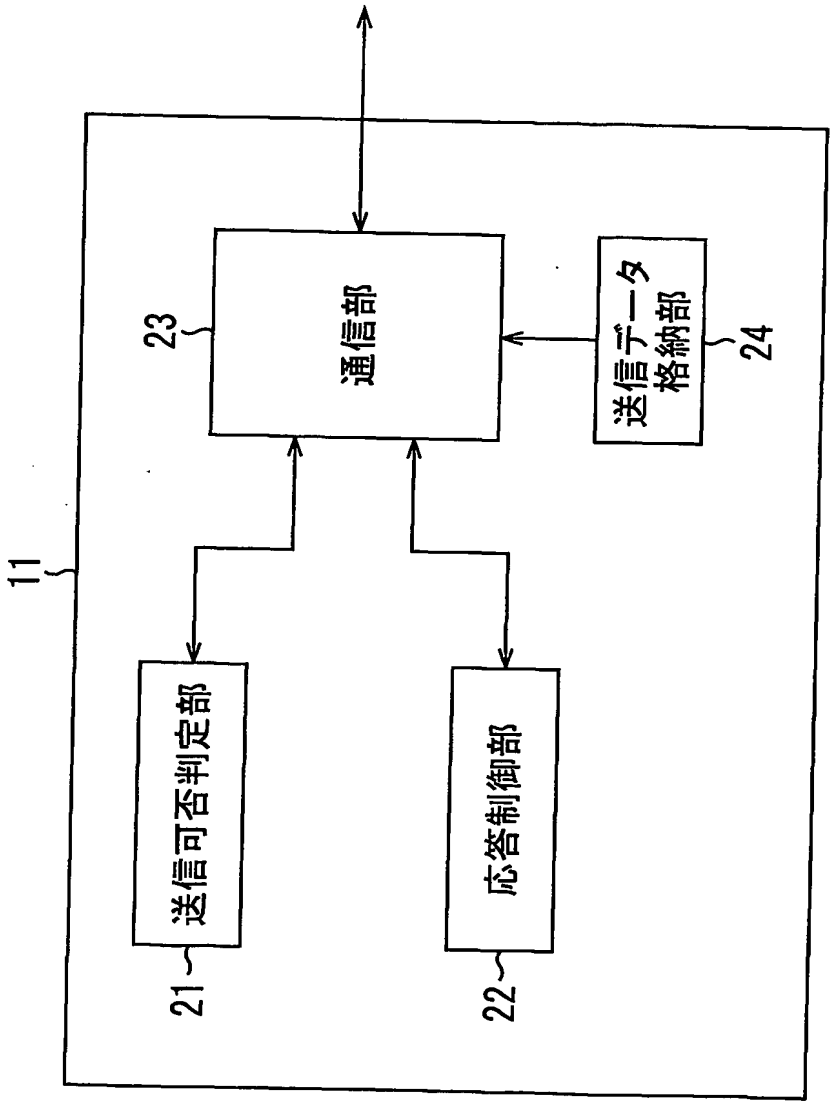


図3

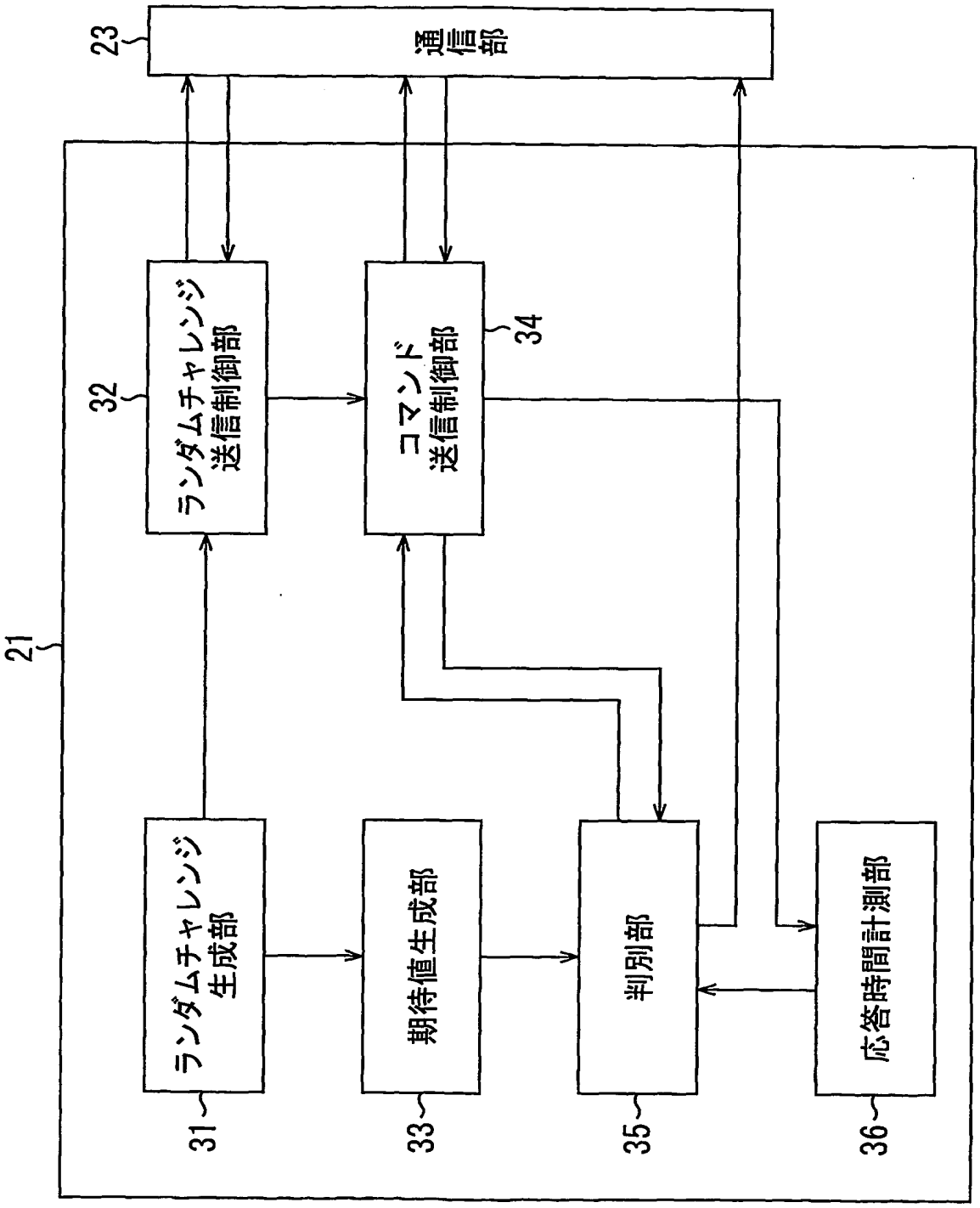

通信部
23
ランダムチャレンジ送信制御部
32
コマンド送信制御部
34
21
ランダムチャレンジ生成部
31
期待値生成部
33
判別部
35
応答時間計測部
36

図4

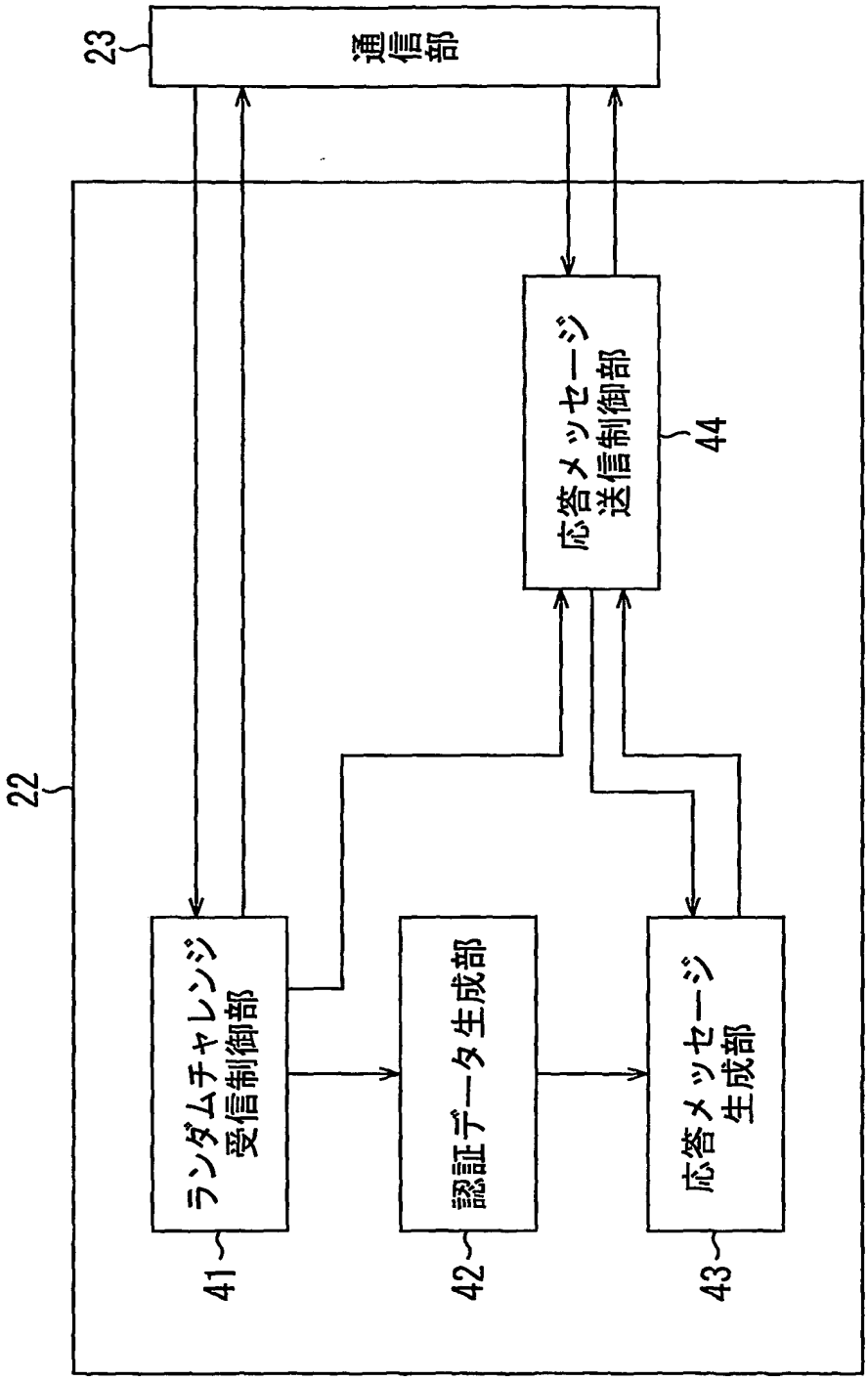

23
通信部
22
応答メッセージ
送信制御部
44
ランダムチャレンジ
受信制御部
41
認証データ生成部
42
応答メッセージ
生成部
43

図５

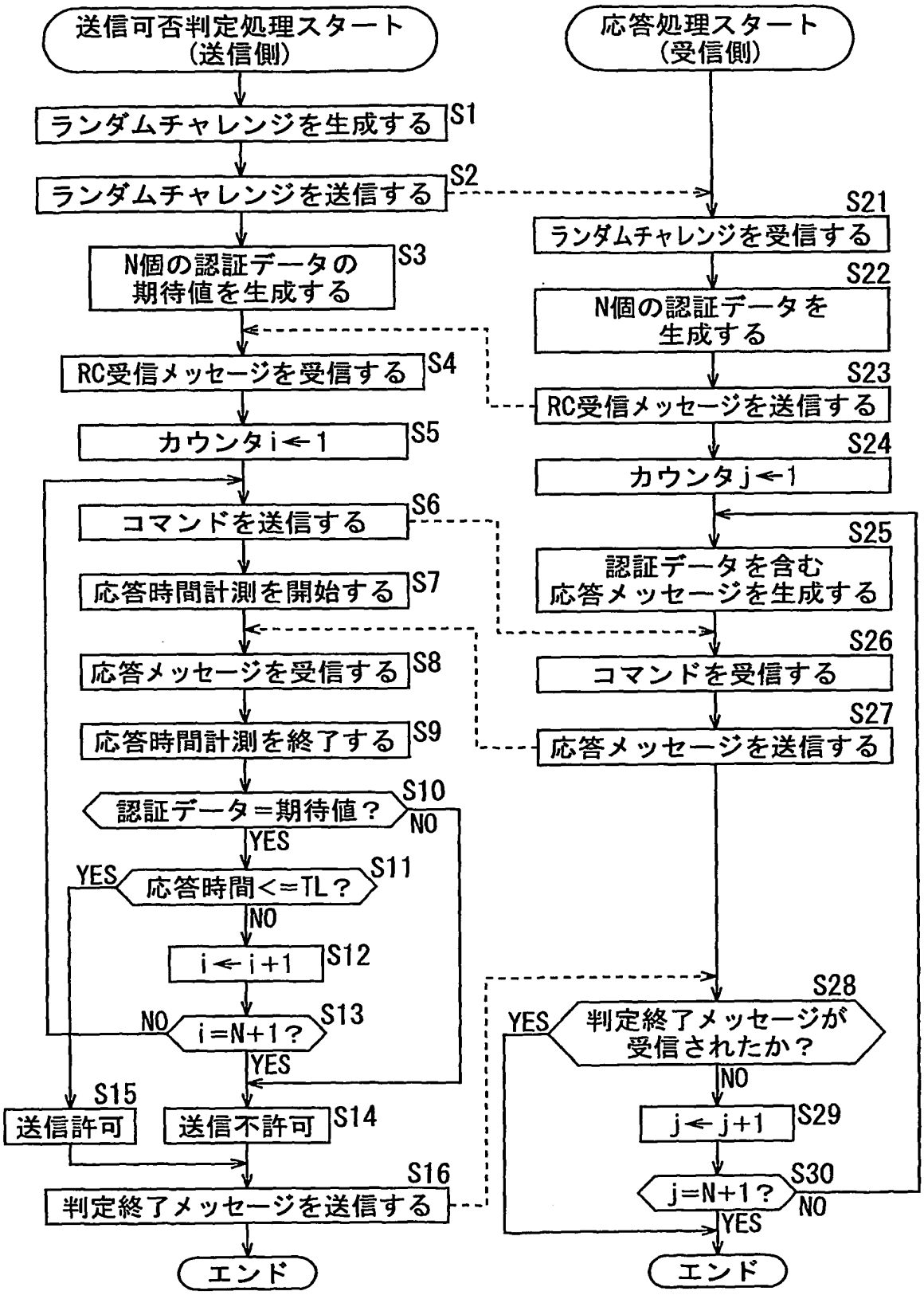

送信可否判定処理スタート
（送信側）
ランダムチャレンジを生成する
S1
ランダムチャレンジを送信する
S2
N個の認証データの
期待値を生成する
S3
RC受信メッセージを受信する
S4
カウンタi←1
S5
コマンドを送信する
S6
応答時間計測を開始する
S7
応答メッセージを受信する
S8
応答時間計測を終了する
S9
認証データ＝期待値？
S10
NO
YES
YES
応答時間<=TL？
S11
NO
i←i+1
S12
NO
i=N+1？
S13
YES
送信許可
S15
送信不許可
S14
判定終了メッセージを送信する
S16
エンド
応答処理スタート
（受信側）
ランダムチャレンジを受信する
S21
N個の認証データを
生成する
S22
RC受信メッセージを送信する
S23
カウンタj←1
S24
認証データを含む
応答メッセージを生成する
S25
コマンドを受信する
S26
応答メッセージを送信する
S27
YES
判定終了メッセージが
受信されたか？
S28
NO
j←j+1
S29
j=N+1？
S30
NO
YES
エンド

図6

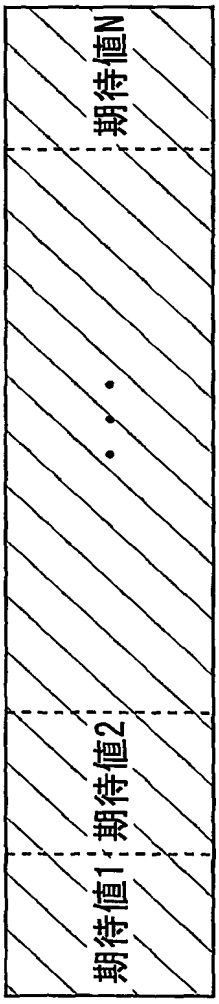


図7

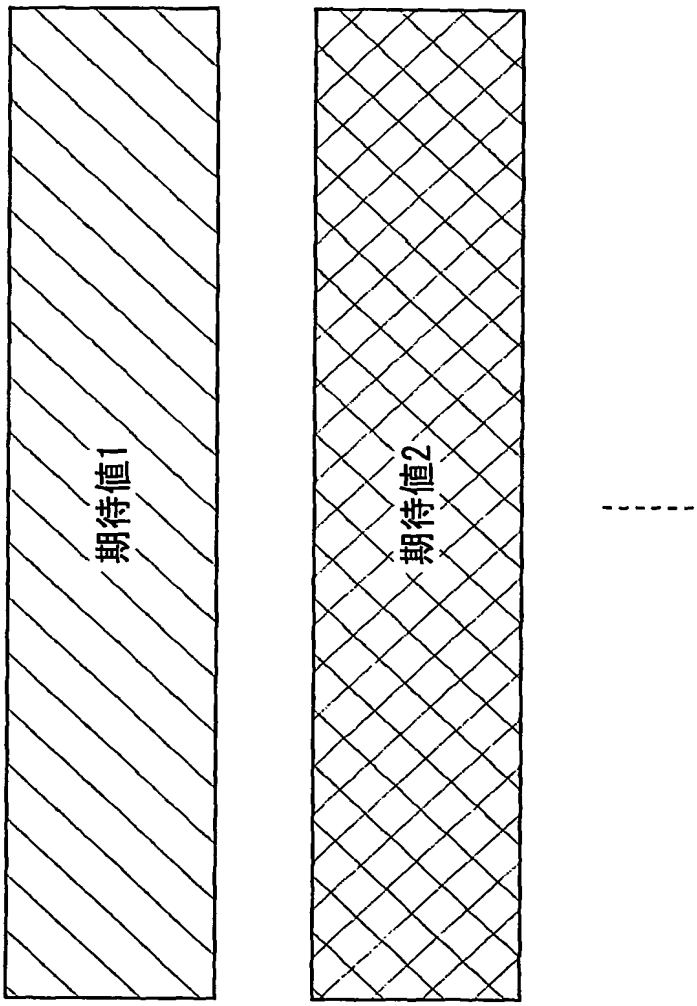


図8

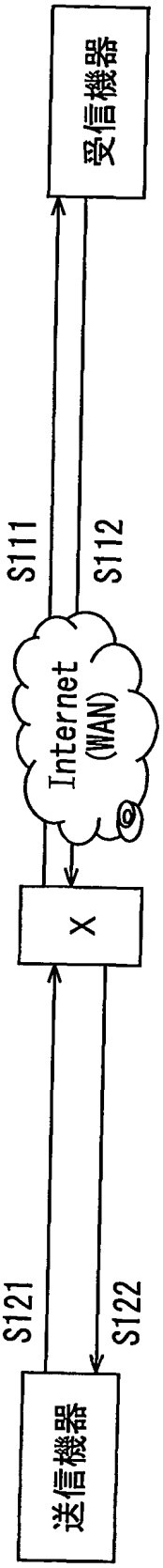


図9

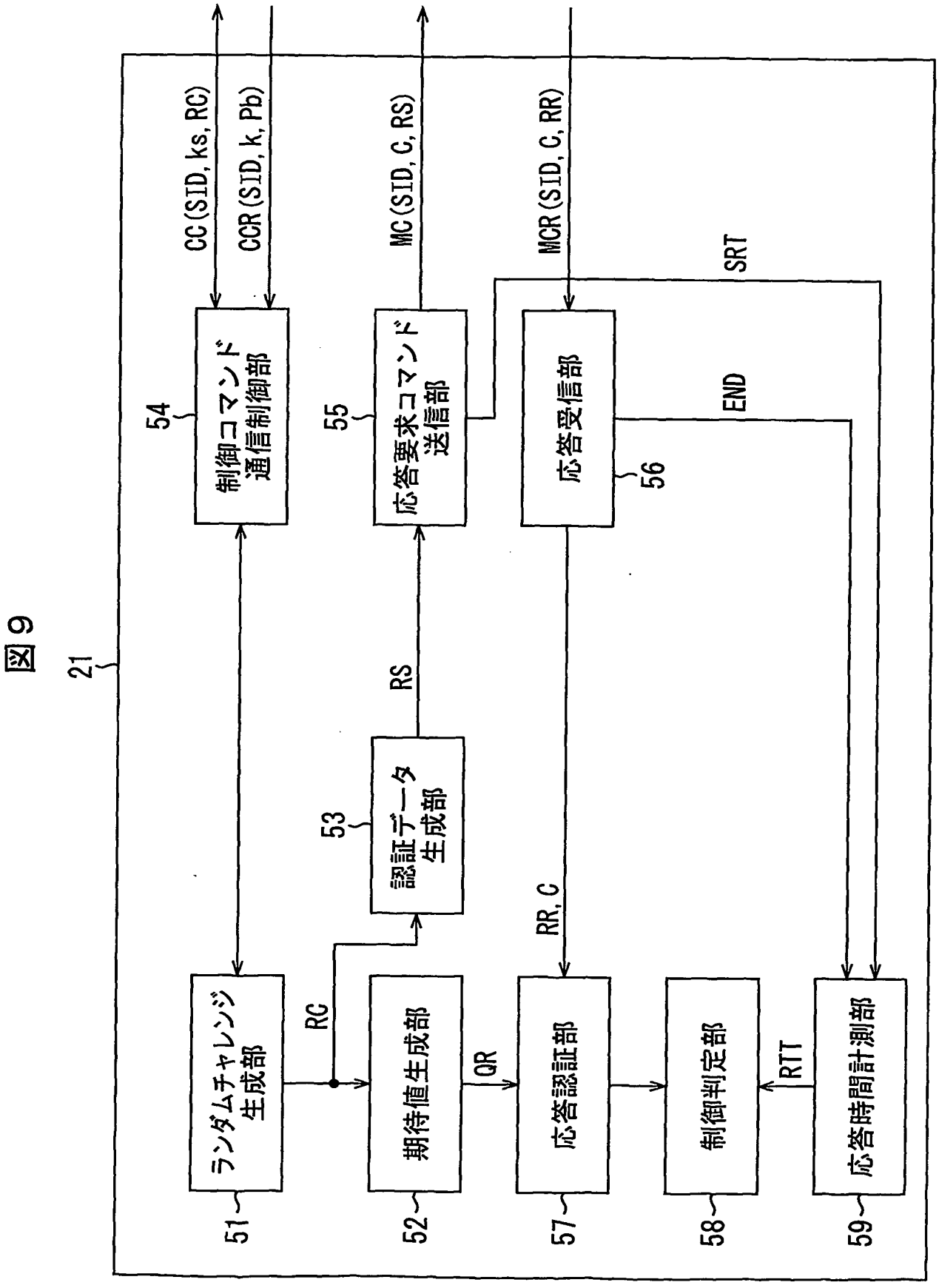

21
CC(SID, ks, RC)
CCR(SID, k, Pb)
MC(SID, C, RS)
MCR(SID, C, RR)
SRT
END
54
制御コマンド
通信制御部
55
応答要求コマンド
送信部
56
応答受信部
RS
53
認証データ
生成部
RR, C
RC
ランダムチャレンジ
生成部
期待値生成部
QR
応答認証部
制御判定部
RTT
応答時間計測部
51
52
57
58
59

図10

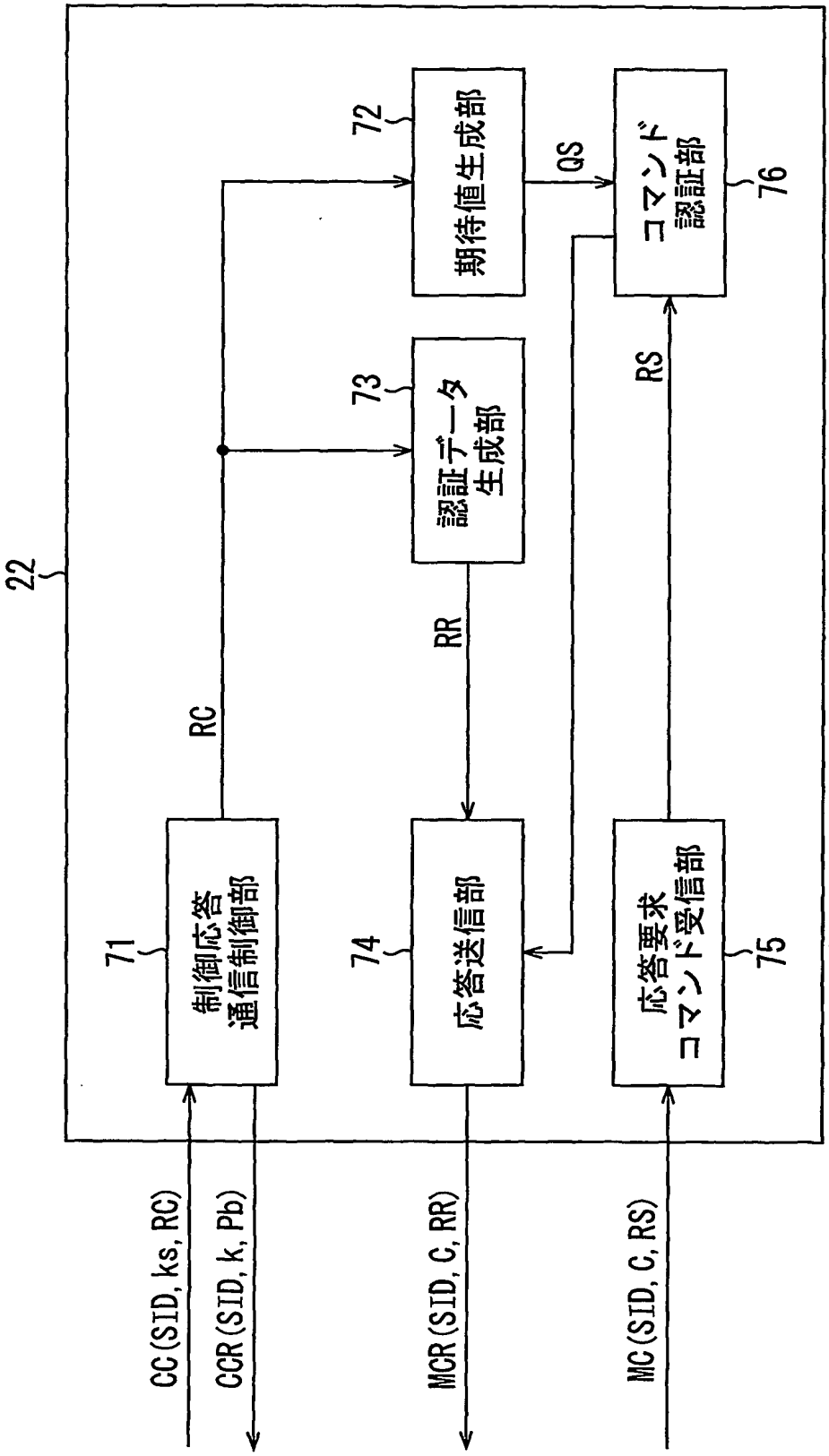

22
71
制御応答
通信制御部
72
期待値生成部
73
認証データ
生成部
74
応答送信部
75
応答要求
コマンド受信部
76
コマンド
認証部
RC
RR
RS
QS
CC(SID, ks, RC)
CCR(SID, k, Pb)
MCR(SID, C, RR)
MC(SID, C, RS)

図11

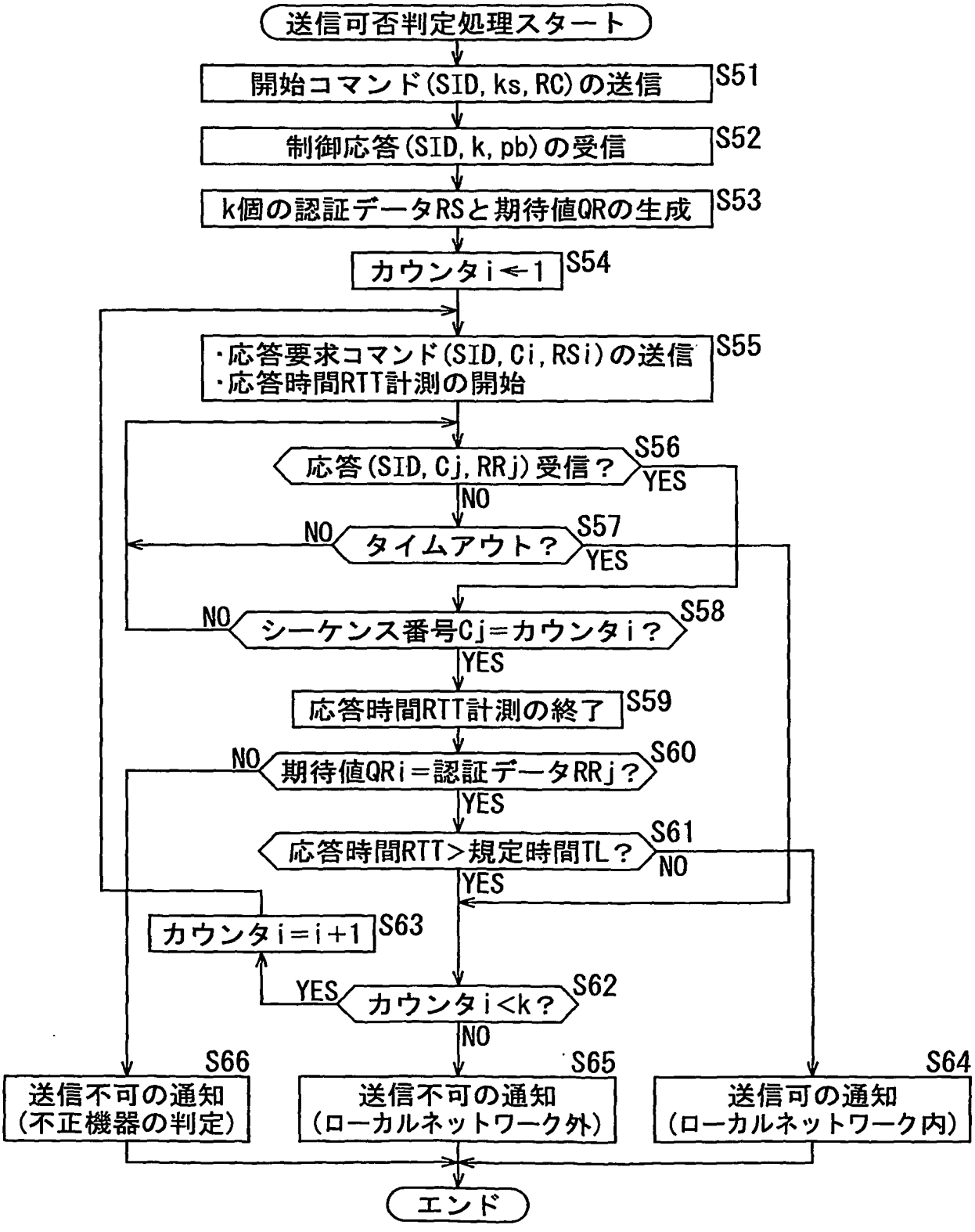

送信可否判定処理スタート
開始コマンド(SID, ks, RC)の送信
S51
制御応答(SID, k, pb)の受信
S52
k個の認証データRSと期待値QRの生成
S53
カウンタi←1
S54
・応答要求コマンド(SID, Ci, RSi)の送信
・応答時間RTT計測の開始
S55
応答(SID, Cj, RRj)受信？
S56
YES
NO
タイムアウト？
S57
NO
YES
シーケンス番号Cj＝カウンタi？
S58
NO
YES
応答時間RTT計測の終了
S59
期待値QRi＝認証データRRj？
S60
NO
YES
応答時間RTT＞規定時間TL？
S61
NO
YES
カウンタi＝i＋1
S63
カウンタi＜k？
S62
YES
NO
送信不可の通知
(不正機器の判定)
S66
送信不可の通知
(ローカルネットワーク外)
S65
送信可の通知
(ローカルネットワーク内)
S64
エンド

図12

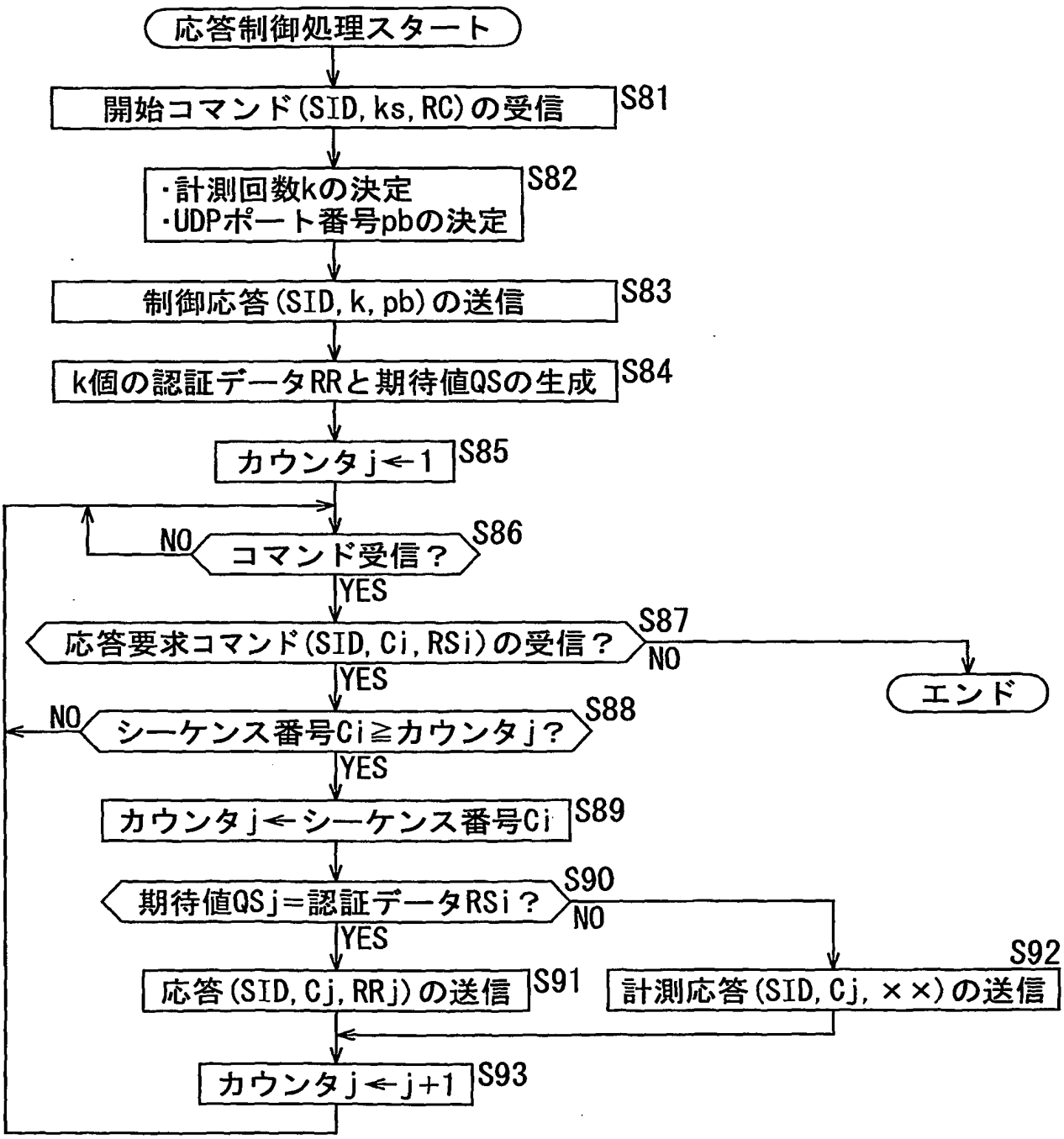

応答制御処理スタート
開始コマンド(SID, ks, RC)の受信
S81
・計測回数kの決定
・UDPポート番号pbの決定
S82
制御応答(SID, k, pb)の送信
S83
k個の認証データRRと期待値QSの生成
S84
カウンタj←1
S85
NO
コマンド受信？
S86
YES
応答要求コマンド(SID, Ci, RSi)の受信？
S87
NO
エンド
YES
NO
シーケンス番号Ci≧カウンタj？
S88
YES
カウンタj←シーケンス番号Ci
S89
期待値QSj＝認証データRSi？
S90
NO
YES
応答(SID, Cj, RRj)の送信
S91
計測応答(SID, Cj, ××)の送信
S92
カウンタj←j+1
S93

図13

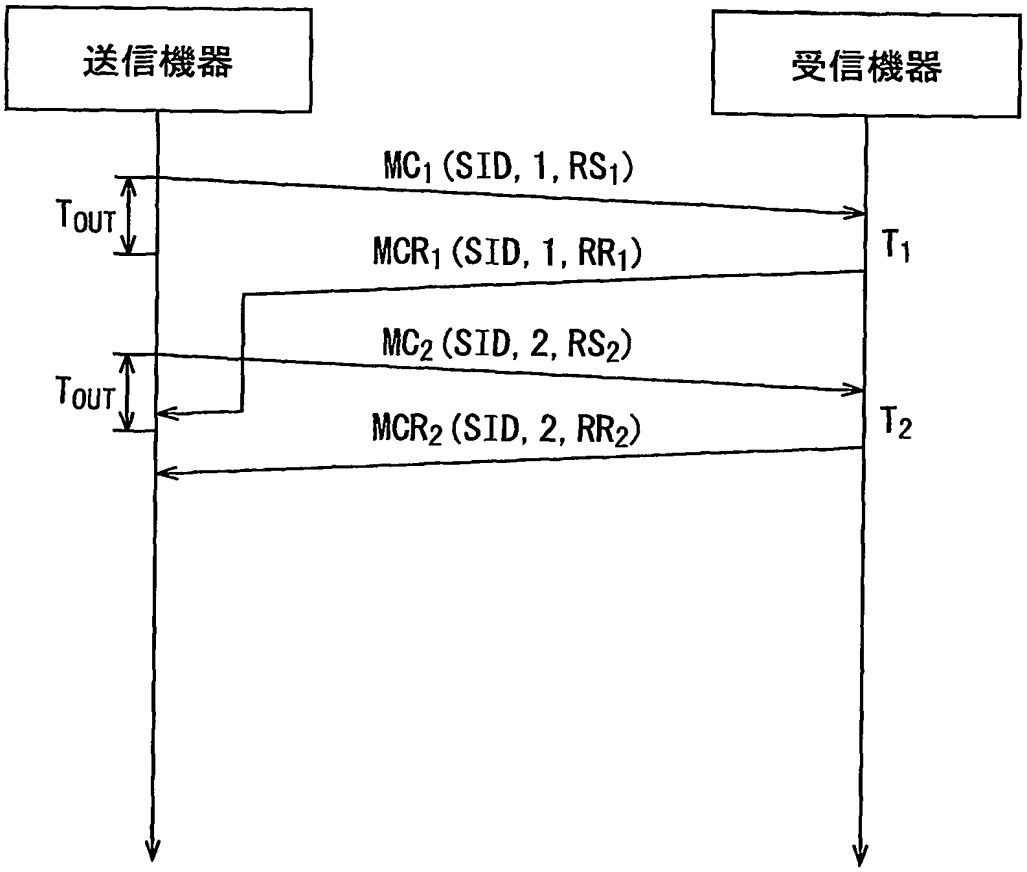

送信機器
受信機器
MC1 (SID, 1, RS1)
TOUT
MCR1 (SID, 1, RR1)
T1
MC2 (SID, 2, RS2)
TOUT
MCR2 (SID, 2, RR2)
T2

図14

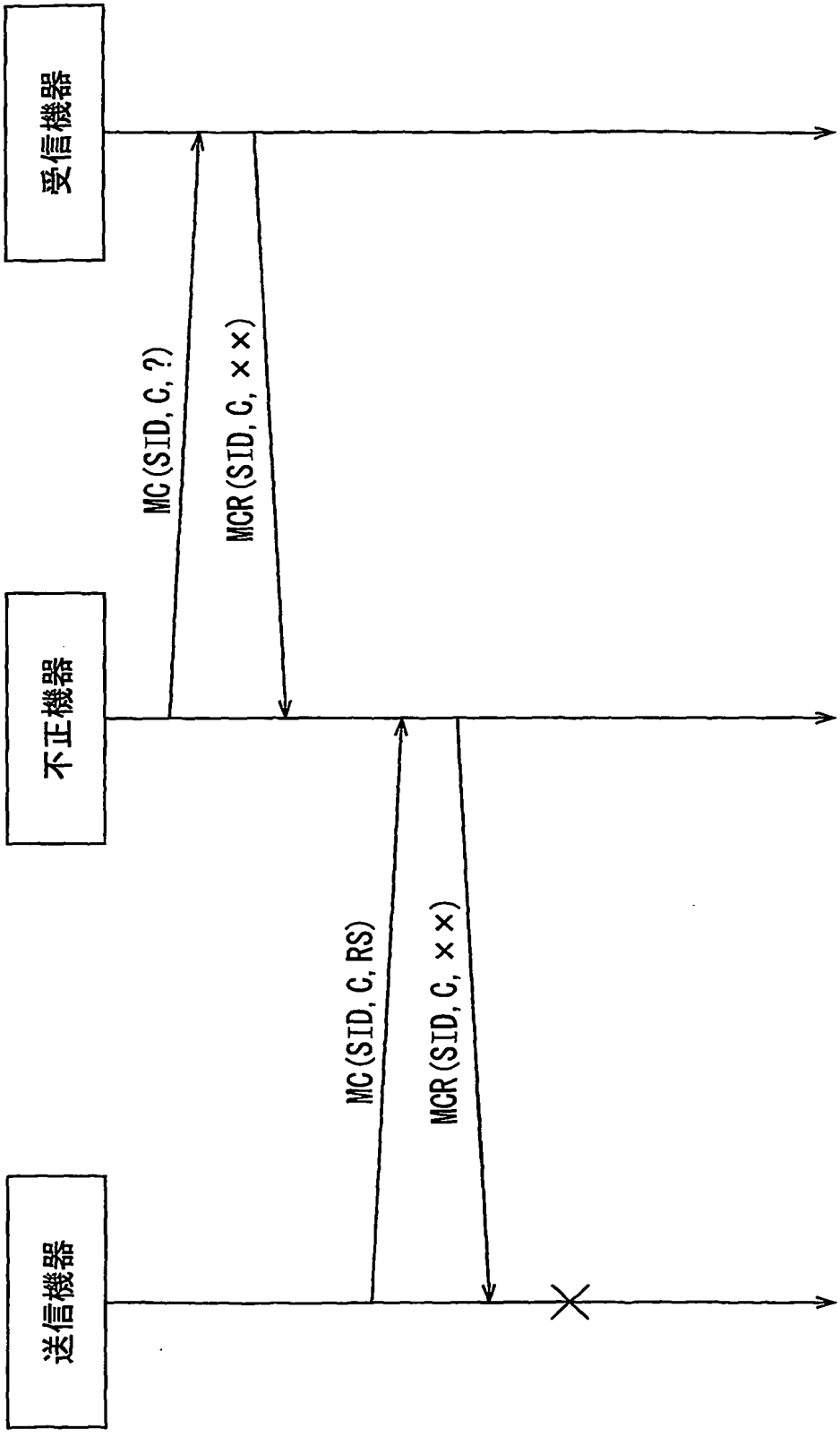


図15

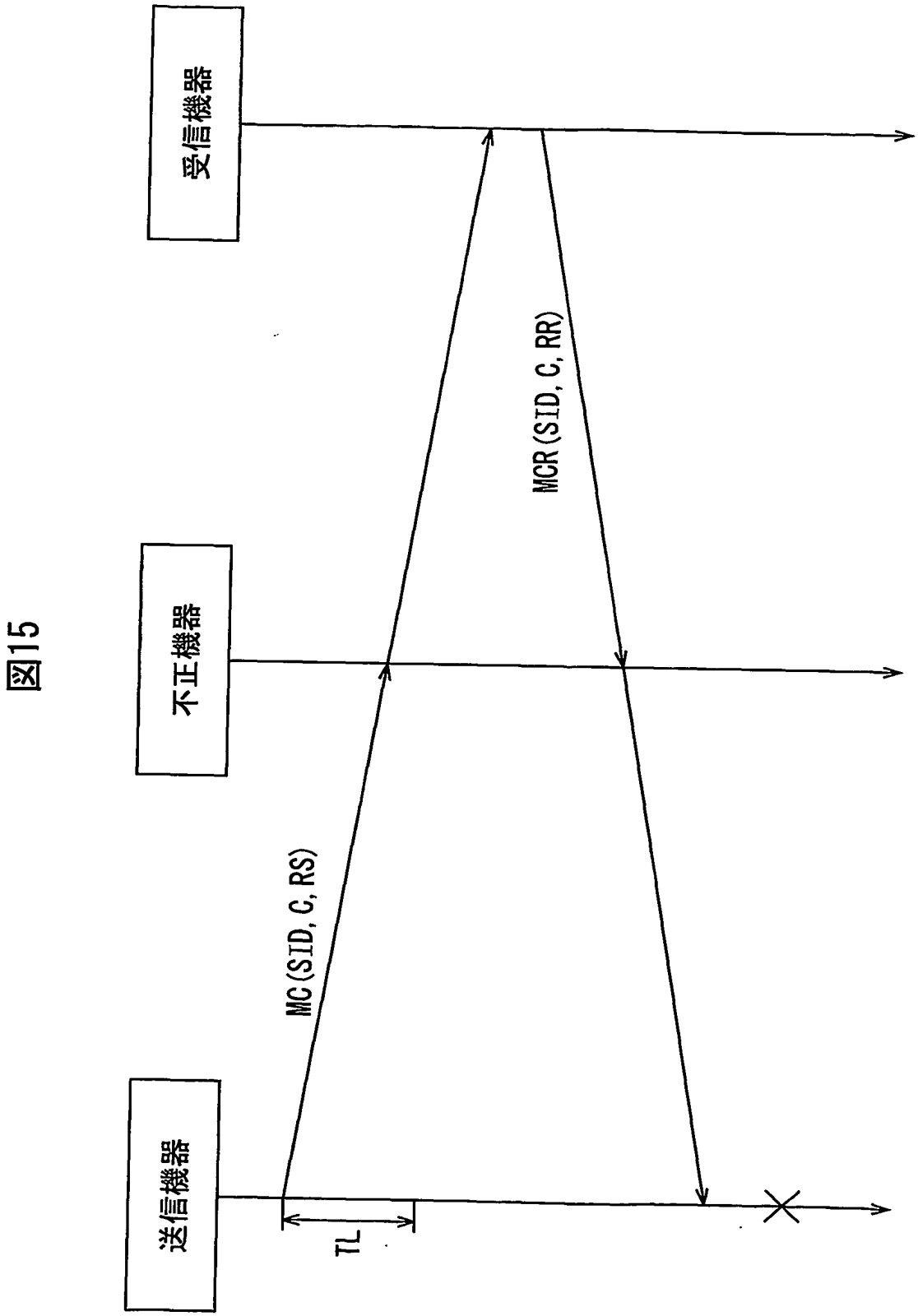
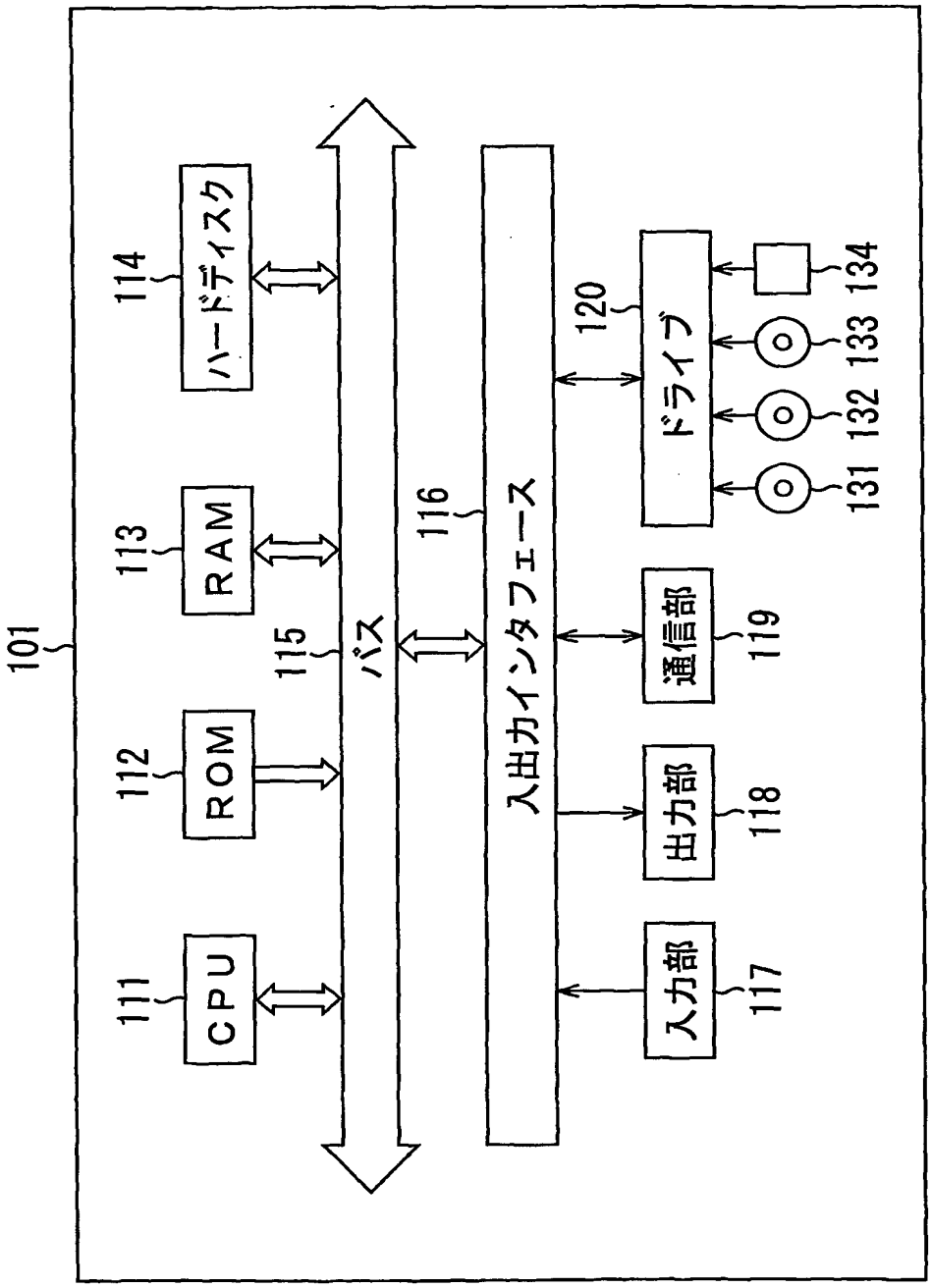


図16


101
CPU
111
ROM
112
RAM
113
ハードディスク
114
バス
115
入出力インタフェース
116
入力部
117
出力部
118
通信部
119
ドライブ
120
131
132
133
134

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/009256

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, H04L9/32, G06F12/14, G06F13/00, H04L12/20

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Toroku Jitsuyo Shinan Koho 1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Ian Fried. 'Apple limits iTunes file sharing'. [online]. CNET News.com.27 May, 2003 (27.05.03), [retrieved on 16 September, 2004 (16.09.04)]. Retrieved from the Internet: <URL: http://news.com.com/2100-1027_3-1010541.html?tag=cd_mh>	1-24
A	Hitachi Ltd. et al. 'Digital Transmission Content Protection Specification Volume 1 Revision 1. 2a(Informational Version)'. [online]. Digital Transmission Licensing Administrator. 25 February, 2002 (25.02.02), [retrieved on 16 September, 2004 (16.09.04)]. Full text, all drawings, Retrieved from the Internet: <URL:http://web.archive.org/web/20030604012332/www.dtcp.com/data/info_dtcp_v1.pdf>	1-24

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 September, 2004 (16.09.04)	05 October, 2004 (05.10.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/009256

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Hachiro ENDO, 'Butsuryu Man no Tameno Pasokon Katsuyo Jissen Koza-96- Network Settei no Kakunin Hoho', MATERIAL FLOW, Kabushiki Kaisha Ryutsu Kenkyusha, 01 June, 2002 (01.06.02), Vol.43, No.5, page 125	1-24
A	JP 11-203249 A (Fuji Xerox Co., Ltd.), 30 July, 1999 (30.07.99), Full text; all drawings (Family: none)	1-24

国際調査報告　　国際出願番号 PCT／JP2004／009256

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ G06F15／00, H04L9／32

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ G06F15／00, H04L9／32, G06F12／14, G06F13／00
H04L12／20

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2004年
日本国実用新案登録公報	1996－2004年
日本国登録実用新案公報	1994－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	Ian Fried.'Apple limits iTunes file sharing'.[online].CNET News.com.2003.05.27.[retrieved on 2004-09-16].Retrieved from the Internet:<URL:http://news.com.com/2100-1027_3-1010541.html?tag=cd_mh>	1-24
A	Hitachi Ltd.他.'Digital Transmission Content Protection Specification Volume 1 Revision 1.2a(Informational Version)'.[online].Digital Transmission Licensing Administrator.2002.02.25.[retrieved on 2004-09-16].全文，全図 Retrieved from the Internet:	1-24

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 16．09．2004	国際調査報告の発送日 05.10.2004
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 宮司　卓佳　5B　9555 電話番号　03－3581－1101　内線　3545

様式PCT／ISA／210（第2ページ）（2004年1月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	<URL:http://web.archive.org/web/20030604012332/www.dtcp.com/data/info_dtcp_v1.pdf>	
A	遠藤八郎，「物流マンのためのパソコン活用実践講座－９６－　ネットワーク設定の確認方法」,MATERIAL FLOW,株式会社流通研究社，2002.06.01，第４３巻，第５号，p.125	1-24
A	JP 11-203249 A(富士ゼロックス株式会社) 1999.07.30,全文,全図(ファミリーなし)	1-24